THE CONDUCT OF WAR IN THE 21ST CENTURY

KINETIC, CONNECTED AND SYNTHETIC

Rob Johnson, Martijn Kitzen and Tim Sweijs

The Conduct of War in the 21st Century

This book examines the key dimensions of 21st century war, and shows that orthodox thinking about war, particularly what it is and how it is fought, needs to be updated.

Accelerating societal, economic, political and technological change affects how we prepare, equip and organise for war, as well as how we conduct war – both in its low-tech and high-tech forms, and whether it is with high intensity or low intensity. The volume examines changes in warfare by investigating the key features of the conduct of war during the first decades of the 21st century. Conceptually centred around the terms 'kinetic', 'connected' and 'synthetic', the analysis delves into a wide range of topics. The contributions discuss hybrid warfare, cyber and influence activities, machine learning and artificial intelligence, the use of armed drones and air power, the implications of the counterinsurgency experiences in Iraq, Afghanistan and Syria, as well as the consequences for law(fare) and decision making.

This work will be of much interest to students of military and strategic studies, security studies and International Relations.

Rob Johnson is the Director of the Changing Character of War Research Centre at the University of Oxford, UK.

Martijn Kitzen is Associate Professor at the Netherlands Defence Academy, Breda.

Tim Sweijs is the Director of Research at The Hague Centre for Strategic Studies and a Senior Research Fellow at the Netherlands Defence Academy.

Routledge Advances in Defence Studies

Routledge Advances in Defence Studies is a multi-disciplinary series examining innovations, disruptions, counter-culture histories, and unconventional approaches to understanding contemporary forms, challenges, logics, frameworks, and technologies of national defence. This is the first series explicitly dedicated to examining the impact of radical change on national security and the construction of theoretical and imagined disruptions to existing structures, practices, and behaviours in the defence community of practice. The purpose of this series is to establish a first-class intellectual home for conceptually challenging and empirically authoritative studies that offer insight, clarity, and sustained focus.

Series editors: Timothy Clack, *University of Oxford, UK,* and Oliver Lewis *Rebellion Defence* and *University of Southern California, USA*

Advisory Board: Tarak Barkawi *London School of Economics, UK* Richard Barrons *Global Strategy Forum, UK* Kari Bingen-Tytler *Georgetown University, USA* Ori Brafman *University of California, Berkeley, USA* Tom Copinger-Symes *British Army, UK* Karen Gibsen *Purdue University, USA* David Gioe *West Point, USA* Rob Johnson *Oxford University, UK* Mara Karlin *John Hopkins University, USA* Tony King *Warwick University, UK* Andrew Sharpe *Centre for Historical and Conflict Research, UK* Suzanne Raine *Cambridge University, UK*

The Conduct of War in the 21st Century
Kinetic, Connected and Synthetic
Edited by Rob Johnson, Martijn Kitzen and Tim Sweijs

For more information about this series, please visit: https://www.routledge.com/Routledge-Advances-in-Defence-Studies/book-series/RAIDS

The Conduct of War in the 21st Century

Kinetic, Connected and Synthetic

Edited by
Rob Johnson,
Martijn Kitzen
and Tim Sweijs

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2021
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

© 2021 selection and editorial matter, Rob Johnson, Martijn Kitzen and Tim Sweijs; individual chapters, the contributors

The right of Rob Johnson, Martijn Kitzen and Tim Sweijs to be identified as the authors of the editorial material, and of the authors for their individual chapters, has been asserted in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Johnson, Robert, 1967– editor. | Kitzen, Martijn, 1978– editor. | Sweijs, Tim, 1981– editor.
Title: The conduct of war in the 21st century : kinetic, connected and synthetic / edited by Rob Johnson, Martijn Kitzen, Tim Sweijs.
Description: Abingdon, Oxon ; New York, NY : Routledge, 2021. | Series: Routledge advances in defence studies | Includes bibliographical references and index.
Identifiers: LCCN 2020041183 (print) | LCCN 2020041184 (ebook) | ISBN 9780367515249 (hardback) | ISBN 9781003054269 (ebook)
Subjects: LCSH: War—History—21st century. | Military art and science—History—21st century.
Classification: LCC U21.2 .C6445 2021 (print) | LCC U21.2 (ebook) | DDC 355.02—dc23
LC record available at https://lccn.loc.gov/2020041183
LC ebook record available at https://lccn.loc.gov/2020041184

ISBN: 978-0-367-51524-9 (hbk)
ISBN: 978-1-003-05426-9 (ebk)

Typeset in Times New Roman
by codeMantra

Contents

List of illustrations ix
List of contributors xi
Foreword xvii
FRANK HOFFMAN

PART I
Introduction: the conduct of war in the 21st century 1

1 Introduction 3
ROB JOHNSON, TIM SWEIJS AND MARTIJN KITZEN

2 Strategic underperformance: the West and three decades of war 17
FRANS OSINGA

PART II
New strategies in the conduct of contemporary warfare 43

3 Hybrid warfare and counter-coercion 45
ROB JOHNSON

4 Strategies for communicating information and disinformation in war: managing and exploiting uncertainty in social media 58
FILIPPO TANSINI AND YAKOV BEN-HAIM

5 Control from the ground up: embedding influence activities in the conduct of war 72
RICK BREEKVELDT AND MARTIJN KITZEN

PART III
New technologies and their impact on warfare 91

6 Humans and hardware: an exploration of blended tactical workflows using John Boyd's OODA loop 93
DAVE BLAIR, JOSEPH O. CHAPA, SCOTT CUOMO AND JULES HURST

7 Cyber countermeasures for democracies at war 116
NORI KATAGIRI

PART IV
War from above 129

8 Air power 2010–2020: from Helmand to Hypersonics 131
JOHNNY STRINGER

9 Armed drones, technological momentum, and the character of war 142
JOHANNES G. POSTMA

PART V
War from the ground up 157

10 The challenge of territory-governing insurgencies on war and peace strategies 159
PAULA CRISTINA ROQUE

11 Security force assistance as a preferred form of 21st century warfare: the unconventional becomes the conventional 173
JAHARA MATISEK AND IVOR WILTENBURG

12 Learning and forgetting counterinsurgency 189
MARTIJN VAN DER VORM

PART VI
Law and war 209

13 Fighting a war without violence: the rules of International Humanitarian Law for military cyber-operations below the threshold of 'attack' 211
BART VAN DEN BOSCH

14 Cyber operations and targeting rules 223
RAÏSSA VAN DEN ESSEN

15 Contemporary urban warfare: does international humanitarian law offer solutions? 236
JEROEN VAN DEN BOOGAARD

16 The conduct of lawfare: the case of the Houthi insurgency in the Yemeni civil war 249
SANDRA DE JONGH AND MARTIJN KITZEN

PART VII
Decision-making and war 265

17 Command in the operational dimension: challenges of the information age 267
ROB JOHNSON

18 The emotions of adversarial interaction 279
LUKAS MILEVSKI

PART VIII
Conclusion: lessons for thinking about war 293

19 Conclusion: assessing change and continuity in the character of war 295
TIM SWEIJS, ROB JOHNSON AND MARTIJN KITZEN

Index 303

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Illustrations

Figures

5.1 Actor/Control Model 77
5.2 Ability to Influence Actors 78
5.3 Proposed Understand, Influence and Effect Framework 80
5.4 Influence Spectrum 81
5.5 Elaborated Understand, Influence and Effect Framework 83
6.1 Performance-Complexity Graph 96
6.2 Kill Chain Placement-Complexity Graph 105

Tables

4.1 Communication Strategy 65
16.1 Lawfare Methods and Outcomes 252

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Contributors

Yakov Ben-Haim initiated and developed info-gap decision theory for modelling and managing severe uncertainty. Info-gap theory is a decision-support tool, providing a methodology for assisting in assessment and selection of policy, strategy, action, or decision in a wide range of disciplines. Info-gap theory has impacted the fundamental understanding of uncertainty in human affairs, and is applied in decision making by scholars and practitioners around the world in engineering, biological conservation, economics, project management, climate change, natural hazard response, national security, medicine and other areas (see info-gap.com). He has been a visiting scholar in many countries and has lectured at universities, technological and medical research institutions, public utilities and central banks. He has published more than 100 articles and six books. He is a professor of mechanical engineering and holds the Yitzhak Moda'i Chair in Technology and Economics at the Technion - Israel Institute of Technology.

Dave Blair is Commander of the 65th Special Operations Squadron, Hurlburt Field, Florida. He is an Evaluator Pilot in the MQ-9 Reaper and the MQ-1 Predator, and an AC-130 Pilot, with combat experience in Iraq, Afghanistan, Syria, and the Horn of Africa. Previously, he served as the Senior SOF Aviation Policy Advisor at the Office of the Secretary of Defense. A graduate of the US Air Force Academy, he holds a Master's in Public Policy from the Harvard Kennedy School, and a Doctorate from Georgetown University, where he studied dark networks. He writes on strategy, technology, leadership, the Royal Navy's suppression of the Atlantic slave trade, the US Coast Guard during Prohibition, and combatting modern-day slavery.

Bart van den Bosch is a Colonel in the Royal Netherlands Army with operational experience from multiple deployments for both United Nations and NATO. He holds a Master's degree in Law and Public Administration as well as a PhD in Law (on the subject of International Humanitarian Law in cyberspace). He currently serves as an associate professor in military law at the Netherlands Defence Academy.

Jeroen van den Boogaard is a senior legal adviser for international law at the Ministry of Foreign Affairs of the Kingdom of the Netherlands and a lecturer and researcher at the University of Amsterdam. Previous working experiences include several positions as a military lawyer of the Royal Netherlands Army; head of the international humanitarian law department of the Netherlands Red Cross, senior legal adviser on administrative law at the Netherlands Ministry of Defence and assistant professor in military law at the Netherlands Defence Academy (NLDA). Jeroen holds a LLM and a PhD in law.

Rick Breekveldt currently serves as a Major in the Netherlands Army Special Operations Forces and is a research fellow at the Netherlands Defence Academy. He holds a Master's degree in Strategic Studies and his research focuses on violent non-state actors. He has recently co-authored Coercion and Non-State Actors: Lessons from the Philippines (2019). Major Breekveldt has served in various command and staff positions at the Netherlands Ministry of Defence, including Army Special Operations Forces, Air Assault and Attack Helicopter units, and he has deployed to Afghanistan multiple times.

Joseph O. Chapa is an officer in the U.S. Air Force and holds a PhD (DPhil) in philosophy from the University of Oxford. His areas of expertise include just war theory, military ethics, and especially the ethics of remote and autonomous weapons. His doctoral research investigates an individual rights-based account of just war theory. He is a senior pilot with more than 1,400 pilot and instructor pilot hours, many of which were flown in support of major U.S. combat and humanitarian operations.

Scott Cuomo is a Marine infantry officer and International Relations PhD candidate participating in the Commandant of the Marine Corps Strategist Program at Georgetown University. He has commanded Marines in combat in Iraq and Afghanistan and deployed throughout other parts of U.S. Central Command, U.S. Africa Command, U.S. European Command, and U.S. Indo-Pacific Command. A graduate of the U.S. Naval Academy, he holds Masters' degrees in National Security Studies from Georgetown University and Operational Studies from the Marine Corps University's School of Advanced Warfighting.

Raïssa van den Essen is a PhD candidate at the Netherlands Defence Academy and the University of Amsterdam. Her research focusses on International Humanitarian Law and the manner in which the rules on targeting govern cyber operations that lack physical effects. She holds a LLM from the Radboud University of Nijmegen and a MSc in Political Science from the University of Amsterdam.

Jules "Jay" Hurst is a Major in the U.S. Army Reserve where he holds the position of a Strategist (FA59). He was formerly a member of the

Algorithmic Warfare Cross-Functional Team (Project Maven) within the Office of the Undersecretary of Defense for Intelligence, the Operations Officer for the U.S. Special Operations Command Analytic Innovation Unit and a Senior Intelligence Analyst within the 75th Ranger Regiment. He holds a Master's degree in Security Studies from Georgetown University and a Bachelor's degree from the College of William and Mary.

Rob Johnson is the Director of the Changing Character of War (CCW) Research Centre at the University of Oxford (www.ccw.ox.ac.uk). His primary research interests are in the history of strategy and war, and their contemporary applications, and he is prominent within professional military education across NATO. He is author of *True to Their Salt* (2017) on partnering, *The Great War and the Middle East* (2016), and co-editor of *At the End of Military Intervention* (2015) and *Before Military Intervention* (2018), as well as several other works on strategy and armed conflicts in the Middle East, Asia and Europe. His leadership of CCW emphasizes the value of blending ideas, theory, and practice in current strategic and security policy.

Sandra de Jongh is a foreign policy professional. She graduated in *International Relations* (MSc, University of Amsterdam) and *Law and Politics of International Security* (LLM, Free University of Amsterdam). The views expressed in her contribution are her own and do not necessarily reflect the official policy or position of her employer.

Nori Katagiri is associate professor of Political Science and Coordinator of International Studies at Saint Louis University. His research interests are in irregular warfare and Asian security affairs, and he is the author of *Adapting to Win: How Insurgents Fight and Defeat Foreign States in War* (University of Pennsylvania Press, 2015) and many journal articles. He has taught at Air War College, USAF, and has been affiliated with Japan's Air Self-Defence Force, US Military Academy at West Point, Taiwan National Defense University, University of the Philippines-Diliman, among other places.

Martijn Kitzen is associate professor of War Studies at the Netherlands Defence Academy. His research and teaching focus on irregular warfare and special operations. In addition to his scholarly work he is, amongst others, involved in (pre-deployment) training for various nations, worked as in-theatre advisor in Afghanistan, and served as academic advisor for the revision of NATO's AJP 3.4.4 (counterinsurgency). Martijn holds a PhD in history, a Master's degree in political science and is a graduate of the Royal Netherlands Military Academy. As a former military officer he has experience in NATO and UN missions.

Jahara 'Franky' Matisek is a mobility pilot, assistant professor of Military and Strategic Studies, U.S. Air Force Academy, and is a two-time

(2018–2019 & 2019–2020) Non-Resident Fellow with the Modern War Institute at West Point, US Military Academy. His primary research interests are in military effectiveness, security force assistance, and how contemporary military strategies vary. He brings an airpower perspective (air, space, and cyber) to the study of old and new battlespaces as a Contributing Editor at the journal, *Over the Horizon: Multi-Domain Operations & Strategies*. In 2019, he was promoted to Lieutenant Colonel as the Director of the Center for Airpower Studies (CAPS), US Air Force Academy. During 2020 he deployed to Afghanistan as a pilot on the E-11 Battlefield Airborne Communications Node (BACN). Dr Matisek has published over 40 articles in peer-reviewed journals and policy relevant outlets, on the topic of strategy and warfare.

Lukas Milevski is assistant professor at Leiden University, where he teaches strategy and security at the BA International Studies and MA International Relations programs. His research interests include strategic theory, the history of strategy and war, and Baltic defense. Dr Milevski has published two books with Oxford University Press, *The Evolution of Modern Grand Strategic Thought* (2016) and *The West's East: Contemporary Baltic Defense in Strategic Perspective* (2018).

Frans Osinga is an Air Commodore in the Royal Netherlands Air Force (RNLAF), Professor of War Studies at Leiden University as well as Chair of the War Studies Department at the Netherlands' Defence Academy. He teaches courses on coercive diplomacy, contemporary warfare and strategy, and peace operations in various BA and MA programs and the Netherlands Defence College. Trained as an F-16 pilot, he is a graduate of the Netherlands Advanced Staff Course, and has studied at the USAF School of Advanced Airpower Studies. His positions include a tour as the MoD Research Fellow at the Clingendael Institute and NATO Allied Command Transformation. He wrote his PhD dissertation at Leiden University on the strategic thought of John Boyd. He is the author of more than 70 articles and co-edited books, including *Military Adaptation in Afghanistan; Targeting: the Challenges of Modern Warfare;* and *Winning Without Killing.*

Johannes G. Postma (Lieutenant Colonel, RNLAF) graduated from the Royal Netherlands Military Academy in 2004 and was commissioned as a fighter controller. Following several operational assignments at the Control and Reporting Center, he served in staff positions at the RNLAF Air Staff to include head of the ISR desk within the C4ISR department and senior policy advisor within the department of plans and policy. Following his time at the Air Staff, he took command of RNLAF Target Support Cell. Lt Col Postma's deployments include a tour as United Nations Military Observer in Sudan and a deployment to the Combined Air Operations Center Al Udeid for Operation Inherent Resolve. Lt Col Postma

holds a MA in American Studies from the University of Groningen, The Netherlands, a MPhil in Strategic Studies from the USAF School of Advanced Air and Space Studies as well as a Master's Degree in Strategic Studies from USAF Air War College.

Paula Cristina Roque is an independent consultant working on conflict analysis. Since 2016 she has been an advisor for Sub-Saharan Africa with the Crisis Management Initiative, a peace-making organization of Nobel laureate and former Finnish President Martti Ahtisaari. She is also a senior external advisor of the South Sudan Centre for Strategic and Policy Studies in Juba. She has a DPhil in International Development from Oxford University where her research focused on the study of two of Africa's strongest and most resilient insurgencies (UNITA in Angola and the SPLM/A in Sudan). She was previously the senior analyst for Southern Africa in 2014–15 with the International Crisis Group. From 2008 to 2010 she was the Horn of Africa senior researcher for the Institute for Security Studies in Pretoria with a focus on Somalia and Sudan. Prior to that she had worked as the China in Africa Research Coordinator for the South African Institute for International Affairs. She is currently writing a book on Angola's Securitised State for Zed Books.

Johnny Stringer is an Air Vice-Marshal in the Royal Air Force which he joined as a university cadet in 1987. He has flown the Jaguar and Typhoon, from junior squadron pilot to station commander of RAF Coningsby. He flew operationally over the former Yugoslavia and to police the Northern Iraq No Fly Zone; staff tours have included the UK Ministry of Defence, and Permanent Joint HQ during the Afghan and Libyan campaigns. He was the UK Air Component Commander in the Middle East during the liberation of Mosul and Raqqah, and is currently Director Strategy at UK Strategic Command. Johnny holds Masters degrees from Oxford and KCL and is a graduate of the UK Advanced and Higher staff courses, and the Royal College of Defence Studies. He has been a visiting research fellow on the Oxford CCW programme in 2011 and 2018.

Tim Sweijs is the director of research at The Hague Centre for Strategic Studies, a senior research fellow at the Netherlands Defence Academy and an affiliate at the Center for International Strategy, Technology and Policy in the Sam Nunn School of International Affairs at the Georgia Institute of Technology. He also serves as an Adviser Technology, Conflict and National Interest to the UK Government's Stabilisation Unit. His main research interest concerns the changing character of modern day conflict. He is the initiator, creator and author of numerous studies, methodologies, and tools for research projects in international and national security risk assessment, early warning, conflict analysis, and strategy and capability development. Tim studied in London, Amsterdam and

Hong Kong and holds degrees in War Studies (PhD, MA), International Relations (Msc), and Philosophy (BA).

Filippo Tansini is an independent scholar and an analyst of SOCMINT (social media intelligence) in the private sector. His research interests mainly focus on strategic and crisis communication, social media dynamics and information warfare, textual criticism and data mining. Dr Tansini's studies have also focused on Early Modern Information Warfare, and the understanding of contemporary Information Operations through the study of Renaissance performative culture.

Martijn van der Vorm is a serving officer in the Royal Netherlands Army. He has been deployed to various counterinsurgency and counter terrorism missions. Currently, he is a PhD candidate at the Netherlands Defence Academy (NLDA). His research focuses on the learning and institutionalization processes of Western armed forces in relation to counterinsurgency operations. Martijn holds a MA in History from Leiden University and a MA in Military Strategic Studies from the NLDA. He co-authored a book on the Dutch Army Special Forces Regiment and its recent operations with Arthur ten Cate (*Callsign Nassau*, Leiden University Press, 2016).

Ivor Wiltenburg is a serving officer in the Royal Netherlands Army. Currently he is conducting PhD research on Security Force Assistance at the Netherlands Defence Academy. He holds MA degrees in Military History (University of Amsterdam) and Military Strategic Studies (NLDA).

Foreword

Frank Hoffman

The late Sir Michael Howard once likened the role of national leaders, those civil and military officials responsible for preparing for future challenges, to that of a 'sailor navigating by dead reckoning. You have left the *terra firma* of the last war and are extrapolating from the experiences of that war'. Howard realized that the greater the distance from the last war, the greater the risk in getting this difficult calculation right. He acknowledged the value of small wars along the way to provide a 'navigational fix' as military institutions sail into 'the fog of peace'. These brief flashes reveal if investments and doctrinal changes are on target.[1] Piercing that fog is no simple matter. As Colin Gray frequently reminded us there is much uncertainty in the world; instead we face an 'inescapable opacity' regarding the future.[2]

The future is certainly opaque, especially to the historically challenged. There are scholars that claim 'we are nearing a point of history where it will be possible to say that war as we know it, long thought to be an inevitable part of the human condition, has disappeared'.[3] Based on some current trends, that author concluded that 'massive, organized conflict is now an exceptional feature of human society, and is on the verge of becoming a historical relic'.[4] Such a conclusion puts a large body of past human experience into the dustbin with little appreciation for its slim evidentiary foundation.

Instead of hubristic nonsense, policy makers need to be re-educated about why and how today's international order was established. Peace and order are not the natural state of international affairs, and long periods of relative stability often induce a state of amnesia about prior periods of political disruption and catastrophic violence.[5] Orders are not sustained without commitments and collective effort. While history never repeats itself, and analogies often betray critical discontinuities, the search for valuable warnings is warranted. The historian Margaret MacMillan, looking back at the onset of World War I, contended that a well-grounded grasp of the past is needed to enhance our awareness of our vulnerability to human error, catastrophe, and sheer accident. As we look ahead to the future, she argued we must remember that:

The past cannot provide us with clear blueprints for how to act, [but] it offers such a multitude of lessons... if we can see past our blinders and take note of the telling parallels between then and now, the ways in which our

world resembles that of a hundred years ago, history does give us valuable warnings.[6]

Professors Hal Brands and Charles Edel reinforce that insight, urging statesmen to study history and adopt a mindset that appreciates the costly lessons of tragedy. Rather than take order for granted, they worry that some 'have forgotten what that order is meant to prevent in the first place: the sort of descent into violence and great-power war that has been all too common thought human history'.[7]

War will remain with us as long as human beings are in charge, and arrange their political and security affairs as nation-states. The weight of history burdens us with its deep continuities when it comes to politics and national security. Change is often abrupt and unpredictable in specific details, but the recurring cycles of tragedy bear close scrutiny and abiding respect. Those charged with advising policy makers or for shaping tomorrow's forces have a special duty to examine the past and glean its harsh lessons with more than a modicum of rigor and prudence.

One of the clearest lessons is the need to avoid 'magical thinking' about technology, and to avoid chasing chimeras like short and painless wars. History reveals the temporary advantage that military relevant technologies confer. Yet, as Oxford's Rob Johnson has noted, 'New technologies, from UAV to robotics, and new methods such as cyber denial of service or disruption, do no more to guarantee victory than did the faith in air and sea power in the early twentieth century. The novelty of a technology has never ensured success in its own right…'.[8] Such technologies are often laminated upon outmoded tactics or misapplied within the wrong organizational structures. Moreover, they may be countered by equally creative adversaries. In theory, the rifled musket and the machine gun made infantry attacks hopeless. Since long-range bombers would always get through and precisely deliver devastating strikes at the key nodes of modern societies, traditional arms were claimed to be irrelevant. The histories of both World Wars, and our own era of protracted contemporary conflicts, have put paid to such visions.

Another lesson involves rigorous intellectual exploration of the future. As scholars of successful military innovation stress, it is not enough for policy makers and senior military officers to embrace a vision of the next war. In addition to this initial intellectual investment, they must generate creative operational concepts as possible solutions, and then 'continue to agonize over such visions to discern how those wars might differ from previous conflicts due to changes in military technology and weaponry, national purposes, and the international security environment'.[9] Critical thinking and a culture that embraces objective experimentation separates the successful from the complacent.

Sir Lawrence Freedman's recent scholarship is apropos. There are many ideas about what the future of war may look like. Some of these are informed and merit being taken seriously, others less so. Professor Freedman

concludes, 'they should all, however, be treated skeptically'.[10] But if we are to fulfill our role as navigators of future security preparedness, we need to be open minded as well as skeptical. Too complacent and one finds oneself at moments like Gettysburg 1863 or the Somme 1916 or France in 1940, when military commanders faced unpleasant options for which their forces were woefully unprepared. Too much enthusiasm about purportedly disruptive technology and indirect modes of warfare may soon leave our military forces too small and poorly postured to deter an ambitious hegemon willing to apply hard power in a decisive manner.

The time has come for some serious 'dead reckoning' from recent events; from Russia's power grab in Ukraine and its bellicose nuclear exercises and brazen saber rattling, and campaign of assassination. The future can be seen in the present, in places like Syria where Iran and Hezbollah's have propped up the Assad regime. Likewise, in the Pacific, the future has been exposed by China's space and missile exercises, its unlawful claims to swathes of the South China Sea, its militarization of lodgments in international waters, and its flaunting of international law and norms. It can also be envisioned by Beijing's assertive diplomacy, its subjugation of Hong Kong, as well as the PLA's sizable military buildup across from Taiwan. Howard's fog of peace is being dissipated, and it is now time to adjust course as the future unfolds.

For these reasons, this wonderful collection of essays is both timely and particularly relevant. The book's intellectual framework of the *kinetic*, *connected* and *synthetic* offers a useful sextant for today's navigators as they explore the outlines of possible armed conflict in the coming years. Each of the contributions in this book afford today's navigators valuable signposts and insights from a diverse set of perspectives and strategic cultures. Policy makers and students of history can avoid the shoals of future crises from these signposts.

Pundits contend that the dynamics of globalization and rampant technological change have unleashed forces we struggle to keep up with, much less envision their significance to security issues. Yet, the *terra firma* of the past reveals the eternal themes and recurring consequences of security dilemmas, rising and declining powers, repressive regimes with predatory ideologies, and weapons that create entirely new domains of warfare. We recognize the enduring continuities of human agency, uncertainty and friction, and primordial forces. The study of that past, as shown in these pages, is the best guide against dangerous speculation and strategic confusion about the future.

Francis G. Hoffman, National Defense University, Washington DC

Notes

1 Michael Howard, 'Military Science in an Age of Peace', *Journal of the Royal United Services Institute* 119:1 (1974), 4.

2 Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Phoenix, 2006), 23.
3 Bruno Tertrais, 'The Demise of Ares: The End of War as We Know It?', *The Washington Quarterly* 35:3 (2012), 7.
4 Ibid., 22.
5 Michael Howard, *The Invention of Peace, Reflections on War and International Order* (New Haven, CT: Yale University Press, 2000), Richard Haass, *The World: A Brief Introduction*, (New York: Penguin, 2020), 303.
6 Margaret MacMillan, *The Rhyme of History, Lessons of the Great War* (Washington, DC: Brookings Institution, 2013), available at http://www.brookings.edu/research/essays/2013/rhyme-of-history.
7 Hal Brands, Charles Edel, *The Lessons of Tragedy: Statecraft and the Preservation of World Order* (New Haven, Yale University Press, 2019), 5–6.
8 Rob Johnson, 'Predicting Future War', *Parameters* 44:1 (2014), 76.
9 Barry Watts, Williamson Murray, 'Military innovation in peace time', in Williamson Murray and Allan Millett, eds., *Military Innovation in the Interwar Period* (New York: Cambridge University Press, 1996), 406.
10 Lawrence Freedman, *The Future of War: A History* (New York: Public Affairs, 2017), 287.

References

Brands, Hal, Edel, Charles, *The Lessons of Tragedy: Statecraft and the Preservation of World Order* (New Haven, CT: Yale University Press, 2019).

Freedman, Lawrence, *The Future of War, A History* (New York: Public Affairs, 2017).

Gray, Colin S., *Another Bloody Century: Future Warfare* (London: Phoenix, 2006).

Haass, Richard, *The World: A Brief Introduction* (New York: Penguin, 2020).

Howard, Michael, 'Military Science in an Age of Peace', *Journal of the Royal United Services Institute* 119:1 (1974), 3–11.

Howard, Michael, *The Invention of Peace, Reflections on War and International Order* (New Haven, CT: Yale University Press, 2000).

Johnson, Rob, 'Predicting Future War', *Parameters* 44:1 (2014), 65–76.

MacMillan, Margaret, *The Rhyme of History, Lessons of the Great War* (Washington, DC: Brookings Institution, 2013), available at http://www.brookings.edu/research/essays/2013/rhyme-of-history

Tertrais, Bruno, 'The Demise of Ares: The End of War as We Know It?', *The Washington Quarterly* 35:3 (2012), 7–22.

Watts, Barry, Murray, Williamson, 'Military Innovation in Peace Time', in *Military Innovation in the Interwar Period*, Murray, Williamson, Milett, Alan, eds., 406 (New York: Cambridge University Press, 1996).

Part I

Introduction

The conduct of war in the 21st century

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1 Introduction

Rob Johnson, Tim Sweijs and Martijn Kitzen

The *Conduct of War in the 21st Century* offers significant changes to the framework of thinking about armed conflict in three respects. First, it updates current thinking on warfighting, weaving together different strands of thought that have emerged in the wake of the conflicts in Afghanistan, Iraq, Libya, and Syria which occurred between 2001 and 2020. Second, it expands upon the conduct of the 21st-century style of war that includes both kinetic and non-kinetic approaches, which is waged both in traditional and in new domains, and which occurs in developed as well as developing polities. Third, it offers new insights into the impact new technologies are having on the conduct of war, including cyber and information, artificial intelligence (AI), unmanned and semi-autonomous systems, satellites, and a new generation of missiles.

This volume is not about the future of war but provides a clear assessment of the lessons that can be derived from the conduct of war in various theatres around the world. The different parts touch on key manifestations of strategy, technology, air power, war from the ground up, law, and decision-making. These salient themes in the execution of contemporary warfare are further explored in chapters that place the relevant developments over the last two decades within the context of the intellectual challenge of thinking about war. The volume thereby examines key dimensions in the conduct of war (the human, the technological, the strategic-operational-tactical, the procedural, and the legal), and shows that our thinking about war, particularly what it is and how it is fought, needs to be updated.

The three cross-cutting key terms around which the volume coheres are *Kinetic*, *Connected*, and *Synthetic*. We examine war as a kinetic activity, applying the original Greek meaning of *kinesis* as pressure, flow, and force, since electronic warfare, just like its physical equivalent, depends on each of these qualities. We investigate the impact of the connected element of war – between peoples, between ideas, through systems, communications, networks, and even across time. Finally, we examine the extent to which war is synthetic, that is seemingly dominated by artificial and manufactured elements, but with an enduring role of the human.

This volume therefore marks a new departure in the study of contemporary war, in that it concentrates on the solutions that have been advanced in theory and practice to deal with the challenges wars have posed in the first decades of the 21st century. It charts the new agenda that has emerged. It is specifically an inter-disciplinary work, brought together by the common and urgent demands created by armed conflict. It is neither a specialised survey of all technologies, nor a staff college guide to current warfighting, since these professional studies already exist. It does not seek to provide an exhaustive overview of all aspects relevant to the conduct of contemporary war. It is, instead, a problematised selection which offers a framework of thinking in combination with critical analyses of the dominant elements that characterise the conduct of war of the first quarter of the 21st century.

Military professionals and scholars share an interest in how to identify and assess change in armed conflict, and, at war colleges across the Western world, they study with great intensity its ways, that is, the actual conduct of war. They are concerned with legal and ethical considerations, the relative utility of force compared with other instruments of power, and new technologies and their impact on how fighting forces and irregular actors make use of them. In 2010, the Oxford Changing Character of War scholars published a volume with Oxford University Press to examine the character of war in past and present conditions, and what emerged was that, despite some changes in the types of actors and their practices (such as the employment of cyber systems), there were striking continuities.[1] In that year, with significant insurgencies against the Western powers and their allies underway, there was perhaps a stronger focus on the violent non-state actor. In the years that followed there were further technological innovations and considerable political and economic changes. These have driven an evolution in the character, if not the nature, of war. At the beginning of the third decade of the 21st century, we are eager to assess what has changed in the conduct of war, and get a better understanding of its emerging characteristics.

A centennial of thinking about the conduct of war

The inspiration for this volume is the work of the inter-war years theorists, between 1919 and 1939, who had begun their deliberations in the aftermath of a significant global war a century ago. They were compelled to reflect on what had occurred but also to consider what lay ahead. Was there a future where international institutions could regulate and even prevent war, or was there the prospect of new and barbaric forms of conflict? They speculated about the impact of new technologies, such as armour, aviation, and wireless communications, and how to harness them. There was widespread concern about the use of poison gas, the prospect of heavy casualties in mechanised land battles, and the widespread destruction of cities by air bombardment. Crucially, these analysts offered a framework of thinking about the conduct of war during a time of considerable political and technological change.

The starting point for this volume, therefore, is J.F.C. 'Boney' Fuller, who was, like some of our authors, a military officer, historian of war, strategic thinker, and advocate of new technological solutions. In 1926, he tried to codify the conduct of war based on an analysis of the global armed conflict that had such a significant impact on his generation, and, two years later, he considered the longer term future of warfare.[2] In most of his 45 books, written across his career, he believed that the purpose of new technologies and original techniques was to create a psychological effect. Herein lies our first connection with the present, for what we see, especially in terms of new technologies, at first seems to herald some breakthrough or a 'revolution in military affairs'. Instead, what is striking is that the use of those technologies is still targeted at, and dependent upon, the endurance, skills, and psychological resilience of the human.

Writing in the Interbellum, Fuller was eager to clarify what could be learned, and applied, from the conduct of war in his own time, and his principles, with some modification, remain in use with modern Western armies. He summed up these principles in three groups: *Control* (the direction of operations and mobility), *Pressure* (concentration of force, surprise, and offensive action), and *Resistance* (distributed forces, endurance, and security). Our approach, building on Fuller, therefore advocates the idea that the character of the current conduct in war is kinetic, connected, and synthetic, with humans still at its core. Fuller's control, pressure, and resistance are applicable to all three of our trinitarian elements. 'Control', in the form of direction, leadership, communications, allocation of resources, or an economy of effort, can be found in each of our elements – in the kinetic aspect of operations, in the connected nature of it, and in the synthetic. Ethical and legal norms considered are all elements of control, and feature in debates on the use of automated systems. Equally, for 'Pressure', we find characteristics in all three of our elements, including the concentration of force in precision kinetic air strikes, in connected cyber disruption operations, and in coercive policies in the so-called grey zone. 'Resistance' appears in all three elements too, in physical kinetic resistance, in connectivity, and in the use of synthetic systems. In other words, we imagine two trinities, one superimposed upon the other, each applicable to the other. We have therefore created a set of three observable characteristics to add to Fuller's original conception, arguing that, in the context of the early 21st century, the grammar of war is kinetic, connected, and synthetic.

Conceptual clarification of the military-human implications of technological change is a connection with this volume, since the advent of new technologies and systems today has created a degree of confusion and uncertainty. This is reflected not only in debates concerning the rules and regulations guiding legitimate conduct *in* war in new domains. State actors' exploitation of an unwillingness to cross the threshold of war, while using violence, disruptive deception, and the speed accorded by information operations, constitutes a serious challenge to the strategic balance.

Considerable strategic experimentation of the past decade, both by state and non-state actors, heralded new forms of contestation, including legal and information contexts, that involve state instruments of influence deployed on and off the battlefield. The accelerated battle rhythm of the second decade of the 20th century also spurred the emergence and the adoption of new forms of command and control that seamlessly exploit high tech tools combined with low tech social forms of organisational adaptation.

The other link between Fuller and our work is manifest as a warning. In Fuller's day, the full potential of the new technologies and the techniques that would optimise them were not embraced by the Western democratic powers but were utilised by their enemies. In Fuller's case, it was the German armed forces that adopted his ideas.[3] It seems clear that a failure to grasp the implications of new technology and the systems that accompany them could profit those who seek to disrupt and defeat the West, and the values the West seeks to uphold, and thus destroy all that was so hard won in the 20th century.

Despite our obsession with the latest technologies and their potential, war is still driven by humans. It is the human dimension that will surely assert itself in war in the near future just as it does in the present. There are plenty of critics of this view. Some technologists and philosophers warn that we may be approaching the end of a period when humans could make the critical decisions, since AI-enabled robotics may have the capacity to replace us. But another way to see this is to remember that humans are a form of technology, that is bio-technology, and it is conceivable that we will see a merging of hardware, software, and human tech, in the same way that humans embraced aviation or mechanisation, creating an almost seamless military instrument in the process. Much of this remains speculation but academic research, as in this volume, can help us navigate these issues based on analyses of how the interaction between human and machines is already reshaping the conduct of war.

Kinetic actors and new strategies: regulars, irregulars, and great powers

The volume reflects on the conflicts of the first two decades of the century. One important element here has been the military role in counterinsurgency and counterterrorism. The 'global war on terror' was led by the military, but critics suggest it should perhaps have been intelligence-led, or law-enforcement led (with extraditions and the co-operation of local security forces), or solely *by, with, and through* local nationals. Direct military intervention by Western armed forces produced protracted insurgencies against perhaps democratically elected, but frail governments fostered by Western powers in Baghdad and Kabul that were unable to establish control over the territories under their nominal dominion. The very small footprint of

Western intervention forces in Iraq following the US withdrawal in 2011 meant that there was little to stop abuses of power, prevent armed unrest, or halt the rise of the so-called Islamic State (IS) in 2014. The insurgent movements that sprung up had draconian rules and systems of governance and could only be halted by force. However, it also became clear that local partners of the West had their own agendas, even when they claimed to be battling a common enemy, showing how the use of locals as surrogates for Western military power can sometimes be misplaced. Yet, the notion that governments of the global south, facing insurgency, can always manage alone also proved to be erroneous.

In the short term, it is governance that must be prioritised to defeat insurgency with the grievances that gave rise to the fighting addressed. The transformative change needed to expunge insurgency is a long-term endeavour, a form of 'nation (re)building', rather than limited 'state building' of institutions. The assistance that can be offered by external powers can take many forms, but the specific military contribution, known collectively as 'security force assistance' or 'security sector reform', has been shown to be far from straightforward. Moreover, offering assistance in the development of a domestic law enforcement or intelligence service has also proven to be problematic. The second decade of the 21st century saw the progressive internationalisation of intrastate conflicts – a quintupling according to Uppsala's Conflict Data Programme – in which external actors intervened in local conflicts for more explicit geopolitical objectives, shifting the focus from stabilisation missions to the strategic and moral vagaries involved in war by proxy.[4] This volume therefore examines how the dynamics of nation building and counterinsurgency missions of the 2000s have morphed into proxy conflicts in the 2010s and considers how third party – state and non-state – actors vie for influence, with deployed kinetic and non-kinetic instruments, to achieve their political objectives.

The 2010s were characterised by a shift towards interstate 'Great Powers' confrontation and the coercion of smaller states. Much would have been recognisable in Fuller's day, but new tools and contexts made the situation by 2020 extremely volatile. The United States and its Western allies have been driven to protect their interests, while China has been guilty of an over-optimism in its ambitions which was interrupted by the global covid pandemic. Russia's policies are driven more by anxiety than ambition, while the emerging countries of the global south are driven more by domestic pressures. While kinetic confrontations are rare, because of the risks involved, the major powers have made more extensive use of other tools to further their respective agendas, including cyber, information campaigns, proxy actors, and an arms race in new technologies. There has been some probing of Western resolve and its defensive systems, usually in situations where the West has failed to avoid resolute or clear responses. Yet there is no doubt that, by 2020, there was an evident confrontation with episodes of coercion underway.

Connected: command, control, communications, surveillance, and information

Command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities are essential to contemporary war fighting. Surprisingly, some aspects of how technological advances in C4ISR are changing the conduct of conflict, and disrupting tactical and strategic actions, remain understudied. Improvements in C4ISR have, for example, driven negative side effects of *strategic compression*, that is, the temptation for senior leaders to micromanage tactical activities on the one hand and the tendency to confuse tactical success with strategic effectiveness on the other. Communications and surveillance capabilities have also led to other developments. We have seen the extensive use of remote and persistently deployable, pervasive intelligence, surveillance, and reconnaissance which link higher headquarters to individual vehicles, airframes, vessels, and squads. Deployable systems with full network access across a greater bandwidth, with the ability to exploit granular data, have been increasingly evident in the battlespaces of the 2010s.

Parallel to this development, there has been renewed focus on information warfare and psychological messaging. In strategic terms, information operations are increasingly conducted against civilian populations through greater connectivity. In the battlespace, information warfare can affect the efficiency of command and control, situational awareness, and the morale of military personnel.

When communications, surveillance, connectivity, and information warfare are combined, they breed a more integrated system of sensors, enablers, and effectors. The boundaries between electronic, space, air, land, and sea domains are slowly but steadily broken down to the extent that all actions are simultaneously tactical and strategic, expanding what was known as the 'operational' dimension. The most prevalent doctrinal trend has been towards accelerated, multi-domain operations.

This has serious implications for the time available for commands. General James Cartwright, former US Vice Chair of the Joint Staff, predicted that 'the decision cycle of the future is not going to be minutes … The decision cycle of the future is going to be microseconds'.[5] Fears that humans will not keep up with the OODA (Observe, Orient, Decide, Act) loop of decision-making are often repeated.[6] The phenomenon has been described as 'hyper-war'.[7] There may be a requirement to devolve command to a far greater extent, to allow subordinates greater license to operate, so as to seize and exploit fleeting opportunities. Still, some tactical events have been conducted at rapid speeds, with negligible effects at the strategic level, and they have not always demanded responses at the same speed from more senior decision-makers. Indeed, tactical events, while moving quickly, can be set in motion to distract an enemy leader who has a preference for interventions in tactical decisions, and this can be subsequently exploited

with more strategic actions. Conceptually, these developments imply a significance for control, pressure, resistance, and flow, and these are perhaps most evident in cyber and electromagnetic operations.

Cyber and electromagnetic activity have been used extensively by state actors but also by violent non-state actors because of relatively low entry costs to achieve tactical effects from afar. This has given rise to more persistent cyber skirmishes, not just in a traditional military sphere, but across the fields of security and defence, which have been barely visible to the public eye, as well as meddling in national information domains, which has gained wider public attention.

In the first decades of the century, the priority has been to see where security might be enhanced against espionage, interference, sabotage by malware, as well as malign information campaigns. Where data is the currency of cyber, so criminal enterprises have sometimes linked up with malign state actors, which, in turn, made clear that extending coalitions and partnerships, across sectors (public and private, military and civilian, nationally and internationally) is the way forward. At the same time, the past period also exposed difficulties associated with speedy attribution of cyberattack and information attack as well as challenges related to containment and proportionate response, and the need to further develop 20th-century concepts of deterrence to make them effective in the cyber domain. These issues, including deterrence through the threat of retaliatory action, through attribution, preparation for certain common types of cyberattack, and the rules regulating targeting practices in cyber space in and outside of war, are examined in this volume.

The synthetic: robotics and artificial intelligence

Autonomous sustainment on land, in the sea, and in the air promises greater mobility and less dependence on lines of communication. Over the past two decades the use of robots and autonomous systems has become more prevalent in conflict theatres around the world. Over a hundred states possess military aerial drones for C4SIR purposes, while at least three dozen of them have weaponised remotely piloted air systems for strike purposes.[8] For ground manoeuvre, multi-role vehicles for clearance or fighting are being developed, while new variants of robotic counter-IED systems have emerged to defeat a new generation of mines. In protection, new armour and lightweight textiles, protective AAD, and counter UAV are already deployed. The implications are that many systems can be automated, reducing manpower demands in combat forces (although technical 'tails' tend to increase), while increasing the mobility and capability of units. Automation also assists in the virtual realm, generating materials, disabling networks, creating new or repairing old networks, enhancing situational awareness, generating deception (especially signals deception), and creating *noise* to conceal communications through replicating tasks.

It is widely believed that future conventional combat will consist of robotic battles, directed by humans.[9] The ability to exploit errors and vulnerabilities in enemy robotics or their command and communications systems will likely also generate precisely the same friction and chance as in previous wars, with episodes of great intensity and destruction followed by periods of stand-off or manoeuvre. Under certain conditions, robotics offer the opportunity to make stealthy insertions, reduce the risk of casualties, conduct persistent monitoring and surveillance. Self-directing underwater and air vehicles, with or without ordnance aboard, can enhance global reach and assist in manoeuvre. Air and ground systems can navigate complex urban terrain while simultaneously monitoring electronic and heat signatures, with greater degrees of accuracy and fidelity. But none of these systems are without technical vulnerabilities. Our volume looks at how unmanned systems and robots have been used in recent battle zones around the world including in the Middle East and North Africa and how they are impacting upon the conduct of war.

Alongside these implications for unmanned systems, the volume also considers how new technologies are reshaping decision cycles. One area of concern that attracts considerable attention is AI. Some see new military opportunities in these assets, while others are more alarmed by its disruption. In simple terms, basic AI is already in service, but strong or adaptive AI remains elusive.[10] AI already assists in identification, problem-solving, pattern recognition, and calculations. But intelligence is characterised as being reactive, predictive, and creative. Currently AI can sense and act, so it is reactive, but its predictive and creative capacities remain limited, especially in the battle space.

All technology is, of course, integral as a weapon or enabler in war but there is often a trade-off in its value and use. At the tactical level, there is evident utility in AI in situational awareness, monitoring, control of loitering systems, and analysis of vast data. The enhancement to analysis offered by AI and automation is well-established, and have immediate military applications in intelligence, navigation, targeting, fire control, communications, and transportation. However, humans are still required to provide the close support, or close quarter combat, of ground war, and will retain the decision-making capacity in most situations, even when AI applications can provide guidance. AI will require built-in safeguards to ensure that errors are minimised, and the ethical standards of war will still apply in situations where AI becomes pervasive. That said, some foresee that the introduction of more sophisticated AI will change the conduct of war, through speed of decisions, responsibilities, and ability to discriminate. Overall, the consensus so far is that AI should not be offered the role of judgement and value, unless risks are low, and judgement should be retained by humans. Our volume examines how military AI applications have reshaped OODA loops in recent conflicts, and how military strategists are pondering its future integration for competitive advantage.

It is striking that human decision-making features as prominently for our authors as the fascination with AI. The challenges of command at the operational and tactical level are well known, in classic warfighting or in problematic insurgencies where there are large numbers of civilians with uncertain allegiances or levels of participation in the conflict. At the strategic level there has been a preponderance of theory but strategic practice is a feature of this work, with studies of how decisions are actually made, including under conditions of deep uncertainty where even the fundamental parameters are not known. Contrasting themes reveal fascinating variations in how to assess and manage change and adaptation, and they tell us much about comparative approaches within Western professional military education.

Framing military thought on the conduct of war

In tracking change across the *kinetic*, the *connected*, and the *synthetic*, we should not forget those aspects of war that always assert themselves. Friction intervenes in conflict. Things go wrong, individuals fail, mechanical systems break down, and attrition imposes itself in all operations, leading to culmination. In its fundamental Clausewitzian elements, war consists of reason, passion, and chance, a 'wonderous' or 'remarkable' trinity in constant tension and therefore prone to unexpected outcomes. Wars involve a variety of actors, each with various agendas or ends which, in conflict, will generate a further set of dynamics. So much of war in the early 20th century would have been recognisable to JFC Fuller: with military personnel grappling with control, pressure, and resistance. In conflicts in the 2000s in Syria, Iraq, Libya, or sub-Saharan Africa, despite the novelty of new and emerging technologies, the elements of the nature of war were present. In Syria and Iraq, for example, the allegiance and the cohesion of the people were important, the political purpose of governance was still extant, and the conflicts were sacralised perhaps even more intensely than those of the 1990s. Did technology determine the outcomes of these conflicts? To some extent it did. Rebels in Syria were overmatched by precise and overwhelming fires, and the belligerents made use of new technological innovations. Yet, on the other hand, resistance to the Syrian regime was not driven by the issue of new technology alone. Few would deny that the human element was still the most significant single aspect of the conflict.

Amongst the comparisons that can be made between war in the industrial age and in the information age, there are several that are conceptually prominent. First, we can observe in particular how, in the past, major powers enjoyed technological supremacy over others, but, periodically, in the conflicts of the early 21st century, there was a degree of parity at the tactical level. Second, in industrial war, information operations were delivered to a well-defined and identifying audience confined to individual states, but in the 21st century the same information was available to a global, critical, and sceptical audience. Third, wars *for* the people now appear to be

wars *amongst* the people. Where wars were defined by allegiance or identity defined by nation states, with distinct ideologies, regionally defined, we now observe increasingly connected peoples, sharing transnational ideas globally, with mass appeal. Fourth, in industrial conflicts, human-speed decisions were the norm, but today, accelerated decisions through an integrated human-electronic interface are common. Finally, there is an emerging global surveillance array, and global strike, which those in previous eras would have found hard to conceive. Current cyber operations are facilitating espionage, disruption, and surprise, but we are seeing code wars with much greater effects, enhanced deception, and stealth, with significant consequences for civilian governance and state integrity.

What has survived from the past is the power of the cognitive and the emotional element in war – another theme reflected upon in this volume based on considerable progress in the cognitive and emotions sciences of the past two decades. The focus of much thinking about war today, just as in the inter-war years, is the psychological element, as influence, subversion, dissonance, or some more extreme shattering of morale.

One of the challenges for the West is how to manage a major operational setback caused by surprise. This is no idle concern: every major war has begun with a major setback for the Western powers. As the recent past indicates, we can anticipate more technological breakthroughs in the next few decades, in robotics, information technology, AI and cognitive science, and materials. These could be combined to achieve persistent C4ISR, deception, greater tactical speed and accuracy, better protection, and a stronger emphasis on air mobility (as other forms of mobility seem likely to remain relatively unchanged). If, however, enhanced fires and communications outstrip manoeuvre and protection, it could produce periods of stalemate and consequently greater attrition. In terms of expected effects, many predict the further compression of time, leaving less room for decision-making at the tactical level and hence a 'hyper war' of dependence on automated systems. Cyberattacks are limited today but it is easy to imagine a much more devastating role for cyber when more and more of the world is connected and dependent on linked systems. Indeed, new forms of connectivity could even promise a *Blitzkrieg* effect, as enemies are left with slow, human-speed systems. Connectivity also enhances the role of subversion and propaganda, eroding confidence in leaders or authorities.

Military thought from the past shows that, while technological-determinist interpretations of war are common, they are not enough to understand war and its evolution.[11] It is easy to refer to new developments in weapons as marking turning points in the conduct of war.[12] All too often, however, technological failures are overlooked.[13] Humans will also find ways to outwit robotics and AI systems, just as surely as they have taken on apparently superior military forces in the past.[14] The singularity of certain technologies or systems can lead to a dangerous over-dependence. For example, advanced air power, whilst influential, did not fulfil the expectations

of its advocates as a conflict-winning weapon system on its own, and 'joint' operations have invariably been the most effective, hence the American interest in 'multi-domain battle'. Technologies confer certain advantages, and may even be essential to selected outcomes, but they do not, on their own, constitute a solution in every case. Their combination with other systems (such as communications), personnel (specialists), techniques (such as tactics), and situation (in, for example, the common objective of a coalition, or part of a grand strategy) is a more certain guarantee of success. Above all, a clear set of goals and an adroit strategy remain fundamental.

The solution to so many of these apparently technical challenges is, as the classic authors of military thought have shown, to return to the centrality of the human in war. The human is the motive force and the point of vulnerability. Despite the advocates of a decisive battle in war, brought about through breaking an adversary, physically and morally, such an outcome is rare in practice and often very costly. Today, we might place greater emphasis on *compelling an enemy to change his mind*. This might be through paralysis, deterrence, disruption or his demoralisation, or might simply be by presenting choices and options, which are themselves shaped, offered, or limited, according to one's strategic intent.

There are measurable strategic designs to achieve the objective of compelling choice. The most obvious, and perhaps over-used as the luxury of the strong, is escalation, and its consequent focus on annihilation or attrition. An alternative is exhaustion (wearing out through time, resources, willingness, or containment). Another is inflexion (to tilt, to manoeuvre, or to seize an opportunity that changes the parameters for the enemy). Yet another is deception (with false fronts, obscuration, multiple axes), or contradiction (where ambiguity, harassment, and multi-tempo actions are used), or reflexion (where one uses the enemy's weight against him, or he is drawn in, goaded, or 'wrong-footed'). There may also be a strategy of persuasion, where allies, partners, and coalitions are formed, diplomacy exercised, and international bodies brought to bear.

To defeat the adversaries of the near future, military forces and their enablers will need to attack the central operating system, namely the mind, just as Fuller already suggested 100 years ago. The routes to do this, and thus compel the target to make a choice which is compliant, can be to induce hesitation or paralysis through fear or confusion; to deter by appealing to an adversary's risk-calculus; to demoralise by depriving the adversary of information, fuel, or health; or to create options that influence their choices and render them predictable. This volume will reiterate that war is a combination of the human, the physical tools, the environments, and the cognitive frameworks. In its conduct, it remains a kinetic activity, in the sense of both physical *force* and the *flow* of information and physical elements. It will certainly be characterised by new synthetic elements – AI, information deception, new materials, and virtual system. Above all, as in the past, war and politics will be about connectivity: human networks,

economic networks, and communicative networks. These elements will reappear in different forms in the future of war, but their nature remains extant. They can be tackled together, combined in various ways, or utilised individually to produce significant changes.

The unifying thread for this volume is therefore an intellectual framework for the *conduct* of war. It is concerned with *how* military and related actions are carried out and how they are understood. Whereas the kinetic, the connected, and the synthetic function as cross-cutting principles for thinking about war, this book, as aforementioned, is divided into different parts that each deal with a germane theme in the conduct of 21st-century war. To aid the reader, the individual chapters each follow the following format: (1) they state clearly the insight offered by the chapter in an opening paragraph, (2) they lay out the intellectual challenge of thinking about war in the context of the chapter, (3) they examine either the human dimension or the technological dimension, or both, and show how the thinking about war is changing, has changed, or requires change, and (4) they then offer concluding reflections that relate to the conduct of armed conflict to illustrate their specific context.

The chapters that follow are scholarly and authoritative, but not exhaustive or artificially theorised, in order to create an accessible interpretation of the conduct of war. They cohere to address the three most fascinating and disputed ideas which are subject to intense debate at this point in the century: namely, the relative impact of those elements of war which are kinetic, synthetic, and connected.

Notes

1 Hew Strachan and Sibylle Scheipers, eds., *The Changing Character of War* (Oxford: Oxford University Press, 2011).
2 J.F.C. Fuller, *The Foundations of the Science of War* (London: Hutchinson and Company, 1926), J.F.C. Fuller, *On Future Warfare* (London: Sifton, Praed & Company, 1928).
3 Fuller himself, no doubt flattered by the accolades he received, entertained proto-Nazi thinking. Fuller was therefore, to a large extent, discredited.
4 Tim Sweijs and Floris Holstege, *Threats Arms and Conflicts: Taking Stock of Interstate Military Competition in Today's World* (The Hague: HCSS, 2020), at https://www.hcss.nl/pub/2018/strategic-monitor-2018-2019/interstate-military-competition/ (Accessed 1 June 2020).
5 Cited in Peter W. Singer, 'Tactical Generals: Leaders, Technology, and the Perils', *Brookings*, 7 July 2009, https://www.brookings.edu/articles/tactical-generals-leaders-technology-and-the-perils/ (Accessed May 2018).
6 Thomas Adams, 'Future Warfare and the Decline of Human Decision-Making,' *Parameters* 31:4 (2001–2002), 57–71.
7 John R. Allen and Amir Husain, 'On Hyperwar,' *Naval Institute Proceedings*, 143:7 (2017).
8 Drones Archive, *Proliferated Drones*, http://drones.cnas.org/drones/ (Accessed 5 November 2019), Peter Bergen, Melissa Salyk-Virk, and David Sterman, 'Who Has What: Countries with Armed Drones', *New America*, https://www.newamerica.org/international-security/reports/world-drones/who-has-what-countries-that-have-conducted-drone-strikes (Accessed 29 June 2020).

9 Peter W. Singer, 'Robots at War: The New Battlefield', in Hew Strachan and Sybille Scheipers, eds., *The Changing Character of War* (Oxford: Oxford University Press, 2011), 333–353.
10 David Schatsky, Craig Muraskin, and Ragu Gurumurthy, 'Demystifying Artificial Intelligence', *Deloitte*, 4 November 2014, https://dupress.deloitte.com/dup-us-en/focus/cognitive-technologies/what-is-cognitive-technology.html (Accessed May 2018).
11 Jeremy Black, 'Determinisms and Other Issues', *Journal of Military History*, 68:4 (2004), 1217–1232.
12 E.C. Sloan, *The Revolution in Military Affairs* (Montreal: McGill University Press, 2002), William Owens, 'The Emerging US System of Systems', *National Defense University Strategic Forum* 63 (1996), W.H. Manthorpe Jr., 'The Emerging Joint System-of-Systems: A Systems Engineering Challenge and Opportunity for APL', *Johns Hopkins APL Technical Digest*, 17:3 (1996), 305–310.
13 Sydney J. Freedberg Jr., 'Artificial Stupidity: Learning to Trust Artificial Intelligence (Sometimes)', *Breaking Defense*, 5 July 2017.
14 Matt Reynolds, 'Sneaky Attacks Trick AIs into Seeing or Hearing What's Not There', *Daily News,* 27 July 2017, https://www.newscientist.com/article/2142059-sneaky-attacks-trick-ais-into-seeing-or-hearing-whats-not-there/ (Accessed May 2018).

References

Adams, Thomas, 'Future Warfare and the Decline of Human Decision-Making,' *Parameters* 31:4 (2001–2002), 57–71.

Allen, John R., and Husain, Amir, 'On Hyperwar', *Naval Institute Proceedings*, 143:7 (2017), https://www.usni.org/magazines/proceedings/2017-07/hyperwar

Bergen, Peter, Salyk-Virk, Melissa, and Sterman, David, 'Who Has What: Countries with Armed Drones', *New America*, https://www.newamerica.org/international-security/reports/world-drones/who-has-what-countries-that-have-conducted-drone-strikes (Accessed 29 June 2020).

Black, Jeremy, 'Determinisms and Other Issues', *Journal of Military History*, 68:4 (2004), 1217–1232.

Drones Archive, *Proliferated Drones*, http://drones.cnas.org/drones/ (Accessed 5 November 2019).

Freedberg Jr., Sydney, J., 'Artificial Stupidity: Learning to Trust Artificial Intelligence (Sometimes)', *Breaking Defense*, 5 July 2017.

Fuller, J.F.C., *On Future Warfare* (London: Sifton, Praed & Company, 1928).

Fuller, J.F.C., *The Foundations of the Science of War* (London: Hutchinson and Company, 1926), https://www.newscientist.com/article/2142059-sneaky-attacks-trick-ais-into-seeing-or-hearing-whats-not-there/ (Accessed May 2018).

Manthorpe Jr., W.H., 'The Emerging Joint System-of-Systems: A Systems Engineering Challenge and Opportunity for APL', *Johns Hopkins APL Technical Digest*, 17:3 (1996), 305–310.

Owens, William, 'The Emerging US System of Systems', *National Defense University Strategic Forum* 63 (1996), https://web.archive.org/web/20100105160638/http://www.ndu.edu/inss/strforum/SF_63/forum63.html

Reynolds, Matt, 'Sneaky Attacks Trick AIs into Seeing or Hearing What's Not there', *Daily News,* 27 July 2017, https://www.newscientist.com/article/2142059-sneaky-attacks-trick-ais-into-seeing-or-hearing-whats-not-there/

Schatsky, David, Muraskin, Craig, and Gurumurthy, Ragu, 'Demystifying Artificial Intelligence', *Deloitte*, 4 November 2014, https://dupress.deloitte.com/-dup-us-en/focus/cognitive-technologies/what-is-cognitive-technology.html (Accessed May 2018).

Singer, Peter W., 'Robots at War: The New Battlefield', in Hew Strachan, Sybille Scheipers, eds., *The Changing Character of War* (Oxford: Oxford University Press, 2011), 333–353.

Singer, Peter W., 'Tactical Generals: Leaders, Technology, and the Perils', *Brookings*, 7 July 2009, https://www.brookings.edu/articles/tactical-generals-leaders-technology-and-the-perils/ (Accessed May 2018).

Sloan, E.C., *The Revolution in Military Affairs* (Montreal: McGill University Press, 2002).

Strachan, Hew, and Scheipers, Sibylle, eds., *The Changing Character of War* (Oxford: Oxford University Press, 2011).

Sweijs, Tim, and Holstege, Floris, *Threats Arms and Conflicts: Taking Stock of Interstate Military Competition in Today's World* (The Hague: HCSS, 2020), https://www.hcss.nl/pub/2018/strategic-monitor-2018-2019/interstate-military-competition/ (Accessed 1 June 2020).

2 Strategic underperformance

The West and three decades of war

Frans Osinga

Introduction

War is, alas, a constant in international affairs. A single look at the news reminds us daily of various conflicts and wars around the world, often persisting for decades. On average, there are 14 UN peacekeeping operations in progress annually involving 110,000 people and around 50 other peace operations carried out by regional security organizations. War is never far away. In fact, cloaked in euphemistic labels such as peacekeeping, humanitarian interventions or stabilization operations, the West has been engaged in three decades of war since the 'outbreak' of peace on 9 November 1989 (the fall of the Berlin Wall). While often stunningly successful operationally, the West has also been repeatedly surprised by the complex operational dynamics it encountered. Despite military superiority political strategic success has often eluded Western military efforts. It struggled to understand the character of contemporary wars.

This chapter aims to explain this paradox, starting with a sketch of the recent Western strategic history. It canvasses in Part II the variety of reasons explaining this strategic underperformance such as the denial of war resulting from a limited understanding of war and the prevailing European strategic culture. Unfounded optimism in the application of new untested concepts and institutional amnesia in the armed forces also played a significant role. In that, however, there is also a paradox as Part III shows; there has been no lack of scholarly interest in modern war often producing strategically relevant pointers that could have and perhaps should have informed strategy and operational planning at the time. Part IV resolves the paradox of this disconnect. Western militaries have been confronted with an expanding array of mission-types that governments could not have expected. Such defence policy fluidity and continued defence spending reductions, hamper organizational learning. Part V concludes with a retrospective mosaic of five images of contemporary war which serves as a warning for thinking about future war and defence policy. While many defence analysts harp on uncertainty, the past three decades actually contain sufficient information to offer a rather sound and prudent perspective on what, as a minimum,

Western militaries can expect and should be prepared for so as to avoid another three decades of strategic underperformance.

Three decades of war: a brief strategic history in three parts

European and US armed forces have been deployed in roughly three dominant strategic contexts, which more or less coincide with three periods: 1990–2001, in which peacekeeping and peace enforcement were central, a period sometimes also referred to as the strategic pause; then 2001–2014, in which the reconstruction of Afghanistan dominated military activities and counter-terrorism became a regular military task; and 2014–2020 where the shock of the Islamic State (IS) and the new assertiveness of Russia forced a rethink.

1990–2001: peace operations in the Balkans

Almost immediately after the fall of the Berlin Wall, civil war broke out in Yugoslavia. The West reluctantly commenced a peace operation to keep the warring parties apart and to force a truce according to the then current classic Blue Helmet model. This model assumed it concerned a conflict between two states, both with a functioning government, that accepted the presence of the peace force which would retain strict neutrality and was only allowed to use force for self-defence.[1] The Blue Helmets therefore had no heavy weapons and any escalation would depend on UN permission to call in air support from Operation Deny Flight. [2]

These turned out to be incorrect assumptions. It was a civil war and the warring parties, Serbs, Croats, Bosniaks and Bosnian Serbs, violated temporary truces when it suited them. There was no peace. So-called Safe Areas, a new and ad hoc concept introduced, proved to be extremely vulnerable and Western politicians were not committed to actually defend these. When air support was requested by Blue Helmets and the UN after a long time threatened to carry out symbolic air strikes, UN observers were frequently taken hostage as a counter-measure, immediately neutralizing the UN threat. Only after the horrors of Srebrenica did a willingness to move from peacekeeping to peace enforcement emerged.[3]

Similar vicious dynamics frustrated NATO in 1998–1999 when it became clear that Milosevic had no intent to end ethnic cleansing in Kosovo. After much diplomatic haggling, NATO countries reached consensus in March 1999 to move to a robust humanitarian intervention in the form of an air offensive, Operation Allied Force. At a tactical level, NATO's professionalism and military superiority were beyond dispute. But the credibility of NATO and the severity of the attacks were unimpressive. The operation hesitantly started at a low intensity. Strategy was marred by disagreement among NATO member states about the types of targets to be attacked and whether escalation was necessary, and by common concern for risks to aircrew and civilian casualties. The targets that were attacked had little actual

political weight with Milosevic. Only when the credibility of NATO itself came into question did political willingness coalesce to escalate, attack more strategically relevant targets, and sustain the operation until Milosevic showed willingness to withdraw his troops from Kosovo.[4]

2001–2014: reconstruction of Afghanistan and COIN

In retrospect, the 1990s were just a strategic 'pause'.[5] The horrific attacks on the Twin Towers and the Pentagon on September 11, 2001 shattered the illusion of security in the West. Where the US proclaimed the global war on terror, Europe preferred statebuilding as a strategic military response, arguing fundamentalist groups found sanctuary in weak and failing states.[6] This liberal statebuilding model, based on Western societies, aspired to create a ring of 'well governed' countries around Europe through the implementation of the rule of law, an effective and representative democratic political system, and the restoration of the security and economy in war torn countries. It called for a joint or 'comprehensive approach': the contribution of and cooperation between military units and other governmental organizations and NGOs.

Statebuilding activities, however, got off to a slow start in both Iraq and Afghanistan. In Afghanistan, the Taliban was able to quickly fill the resulting security gap when it became clear that the international force was far too small to exert influence all over Afghanistan. Statebuilding requires security but the increasing threat of Improvised Explosive Devices and ambushes necessitated prioritizing protection of own troops and fighting an assortment of irregular fighters. While successful on a tactical level, these actions also slowed down the pace of reconstruction activities. From 2007 it had to be recognized that NATO faced an insurgency. The answer was a rediscovery of counterinsurgency (COIN), a combat mission, an unwelcome message for politicians in Germany and the Netherlands, for example, and a task Western armed forces were unprepared for: knowledge and expertise in irregular warfare were lacking. Fighting such adaptive opponents was also extremely complex due to the many restrictions imposed on Western units regarding the use of force.[7] The mission ended in 2014. Afghanistan is still not stable, witness the frequent bomb attacks there.

2014: Russia and the rediscovery of collective defence

That year followed a geopolitical shock, the annexation of Crimea by Russia. It was a watershed moment.[8] In 2010, the NATO Strategic Concept considered interstate threats near the NATO treaty area very unlikely. Yet, from 2014, the new rivalry with an assertive Russia became the central strategic problem again presenting Europe with three strategic challenges: (1) hybrid warfare, (2) the rediscovery of conventional deterrence and (3) the rediscovery of nuclear strategy.

Hybrid warfare, the Western label for Russian actions during the annexation of Crimea, refers to the orchestrated deployment of subversive activities, psychological warfare, media manipulation, deception activities, cyberattacks and intimidation of politicians. It aims to exert influence without applying overt military force, remaining deliberately below the threshold of violence of the Western concept of war. It is the zone between peace and war. While a time-honoured stratagem, the West had lost sight of it and was also surprised by the impressive military modernization of fighters, tanks, anti-aircraft systems, and surface-to-surface missiles, cyber capabilities and electronic warfare assets coupled with demonstrations of large-scale exercises – 'snap exercises' – in which sometimes more than 100,000 troops moved quickly over strategic distances, presenting an intimidating threat to Eastern European NATO member states. The shock was reinforced by the recognition that the credibility of the conventional deterrence of the West, and thus the collective security concept of NATO, was in doubt as Europe had long lost capabilities and expertise for high intensity warfare. This also applied to the nuclear dimension.[9] While Russia is prepared for a (limited) nuclear war in Europe there has hardly been any discourse about nuclear deterrence since 1990. As more than one report concluded, NATO does not have an adequate response to a Russian escalation, a sobering observation for the Baltic States.[10]

If we accept that the three decades of war started with George Bush's call for striving towards a new and liberal world order in 1990, subsequent interventions, while motivated by laudable humanitarian concerns, can be considered wars for expansion and maintenance of the liberal world order. Undeniably, the three decades' war saw remarkable tactical military performances, innovative operational concepts, demonstrations of military superiority and an unprecedented ability to reduce the risk not only for Western military personnel but also that of civilian casualties and collateral damage. Moreover, peacekeeping operations generally did alleviate human suffering, after a while and for a while (many wars have flared up after initial peacekeeping success). However, while toppling authoritarian regimes was achieved at remarkable low costs, the aftermaths of such societal upheaval in Iraq and Libya has proven to be catastrophic for the people and the wider region. And interventions in Afghanistan and Iraq have been very costly in financial terms and in lives lost, and have not produced the long-term stability and societal transformation so desired. At the dawn of the third decade of the 21st Century, one must conclude that the Western use of military force underperformed strategically.

Explaining the strategic underperformance

Many explanations for these military-strategic problems have been advanced. First, the exceptional strategic culture that prevailed within Western European societies. The military instrument had lost its value and

legitimacy, and, as John Mueller argued, by 1989 major war had become sub-rationally unthinkable in the West. Soft power – the positive effect of globalization, liberalism, international treaties and organizations – was considered more important in the future than hard power. Europe was safe. Only humanitarian operations justified investment in defence.[11] Instead of war, these were labelled with terms such as peacekeeping operations, training missions, reconstruction missions, or humanitarian interventions, even though the actual operational dynamics no longer matched these euphemistic labels. War had 'disappeared' from the societal frame of reference.[12] 'Europe lives on Venus, America on Mars', argued Robert Kagan in his acclaimed book *Of Paradise and Power*, raising a warning finger towards Europe.[13]

This was an optimistic denial of history indeed and also removed understanding of the strategic logic of the vicious dynamics in which military units entered, and of what Western military units were actually concerned with. And that was waging war in the famous Clausewitzian sense: trying to impose the will on an opponent by military means. Europe's limited view became apparent in the Balkans and Rwanda, for instance, where ethnic cleansing, political massacres and rapes as a barbaric by-product were not recognized as integral parts of a targeted warfighting strategy of the warring parties. The limited legalistic Western perspective on what war is, when and how it can be waged, by whom and against whom, also blinded many in 2014 during the annexation of Crimea: there was no clash between two armies and hence did not resemble the paradigmatic image of war.

A second factor concerns risk aversion: a central feature of Western strategic culture is the almost obsessive concern about risks to military personnel, but especially for collateral damage and civilian casualties. This is partly because the use of precision weapons in various missions managed to limit these risks to a historically unprecedented low level which as a result became the political and ethical norm and expectation. This in itself is a valuable development. Christopher Coker called the Western way of war 'Humane Warfare', because it was accompanied by an unprecedented respect for the law of armed conflict and because the West only waged war over humanitarian interests, or at least could justify an intervention in that way. However, if civilian casualties were to be regretted, this could lead to critical media and political questions about the legitimacy and effectiveness of the operation. Such sensitivity to risks translated into stringent restrictions on the use of force during missions and often an unrealistic emphasis on protecting both forces and civilians.[14] Opponents of all kinds, such as Karadzic, Saddam Hussein, Mullah Omar, and Gaddafi, have exploited this sensitivity to the full.

A third factor might be termed strategic fuzziness, namely the denial of war has also been accompanied by neglect of the associated strategic frame of reference, resulting in virtual strategic illiteracy and a decline of strategy.[15] Basic principles of military strategic thinking have frequently been

ignored or, in any case, have been less prevalent over other considerations. For example, during Operations Deliberate Force and Allied Force, not strategy dictated the plan of attack, but a list of targets that NATO member states could agree on after a consensus seeking political process regardless whether these actually represented politically relevant coercive value.[16] In Afghanistan there was no strategy.[17] Fighting the Taliban, itself a necessary tactical activity, filled the gap, Hew Strachan concluded.[18] This also applied to the concept of the Comprehensive Approach, the 3D approach which took the place of strategy, but was merely an inward-looking organizational concept that had never really proven itself and faltered in implementation because the participating non-military organizations did not necessarily have the same objectives or level of commitment, nor sufficient capabilities, nor the willingness to align their activities with military units.[19] As during the various Balkan crises, lack of unity among Western states also affected Operation Unified Protector in 2011 and mounted a serious coherent response towards Russia in 2014.

Fourth, missions often featured ill-defined objectives and mission creep; the mission increased in size, aims and complexity. In the Balkans, Blue Helmets had to initially observe truces, escort convoys, then contain violence, and guard (but not protect) safe areas and, eventually, to force the leaders of the warring parties to the negotiating table. Exactly what success entailed was not always evident or measurable with common military criteria. The utility of force, Rupert Smith argued, is no longer about winning a victory but creating a condition in which a political solution can be sought.[20] While true, that offers little guidance to military personnel. In Afghanistan and Iraq, ISAF pursued 'maximalist' objectives: the complete redesign and reconstruction of a neo-patrimonial conservative and politically corrupt society that was not Western-oriented and had no tradition of effective state administration according to Western democratic model. Diligent efforts were made to find criteria that could provide insight into the stability of a country, improving the legal system or setting up an accountable governmental structure but how do you measure success if the objective is to rebuild an entire society or a province?[21] Moreover, the objectives could differ between contributing member states.[22] Merely participating in the mission was the primary political goal for many countries. Finally, the resources made available were often not in line with the objective, size and complexity of a mission. In the Balkans, the UN never got the 36,000 blue helmets needed in the first few years. In Afghanistan it proved difficult to generate sufficient international contributions. COIN and statebuilding missions require a large force and a long breath. Even when ISAF was finally 130,000 strong, this proved insufficient for such a large area against a tenacious and tough Taliban.[23] 'Unwinnable' as Theo Farrell titled his study on the British deployment in Afghanistan.[24]

Finally, misperceptions, knowledge gaps and institutional amnesia have been important strategic problems. First, the planning of the initial peace

operations in the Balkans erroneously assumed that the civil wars there had strong similarities to previous conflicts in which classical peace operations were conducted. Second, the armed forces and academic institutions had little knowledge of the nature of these civil wars, their motives, their origins and the logic of violence employed by warring parties. Third, there was hardly any knowledge about the dynamics of coercive diplomacy: the question of how, with limited resources, one can credibly impose one's will on an opponent and force it to make concessions or stop its actions. Fourth, an unfounded optimism about the success of sometimes still untested strategic concepts. The mission in Afghanistan was undertaken without empirical evidence to support the idea that the liberal statebuilding model could be successfully implemented in a fragmented non-Western country.[25] Finally, institutional amnesia: knowledge and expertise had been lost on counterinsurgency, and, as became evident in 2014 in many European states, also on high intensity interstate warfare, including nuclear deterrence.

The paradox: a vibrant study of war

The paradox is that there was no shortage of growing insights into strategic issues. Indeed, the study of war flourished, precisely because of the strategic and operational problems that Western armed forces encountered, as a brief and selective sketch of the intellectual landscape will show. Desert Storm inspired a heated debate about the significance of it for the future of Western warfare.[26] One camp argued a Revolution in Military Affairs was taking shape. New precision weapons, stealth fighters, cruise missiles, electronic warfare systems, new sensor platforms, all connected by data links, yielded an unprecedentedly effective force capable of defeating Iraq (the world's fourth army at the time) without incurring major losses. These new technologies led to new operational concepts such as Network Centric Warfare and, what has come to be called, the New American Way of War: the use of precision weapons, optimal use of air superiority and, if possible, avoiding ground troops in direct combat with the opponent.

In academic circles, these new technologies and the Balkan challenges led to a rediscovery of the theory of coercive diplomacy and deterrence.[27] How can a leader like Milosevic be forced to accept the demands of the West with only limited use of military force? What political preconditions should be kept in mind? Which target complexes should be threatened or attacked, and how intensively, to exert effective political pressure? What new strategic opportunities did precision weapons offer? And above all, what explained the failures of Western conventional deterrence?[28]

European analysts doubted Desert Storm's relevance because such a war no longer seemed likely. Studies instead focused on the role of violence in peace operations and the limits of the classic Blue Helmets model, leading to suggestions for 'wider peacekeeping' and 'robust peacekeeping' and, after the horrors of Srebrenica and Rwanda, to the development of the peace

enforcement concept.[29] Critical studies examined to what extent humanitarian interventions could actually end civil wars arguing that controlling violence often seems feasible, provided that UN troops remain in a conflict region for a long time. Tackling the root causes hardly appeared possible. Others advocated intensifying humanitarian interventions. Sovereignty should no longer be an obstacle to intervene when a regime oppresses its own population.[30]

Other studies focused on the nature of the civil wars, arguing these were 'New Wars' that could not be understood from the Western instrumental strategic perspective. New types of warlords were not seeking peace; they exist in a mutual parasitic-symbiotic relationship to continue the local war in order for each to maintain their position of power. War is an end in itself and peace is not desirable. Others discussed whether 'old hatreds' were the causes, or economic deprivation. A third category pointed to the instrumental role that ethnicity, religion and nationalism play in civil wars demonstrating how leaders can mobilize religion, ethnicity, myths and symbols to create enemy images and gradually legitimize extreme violence against 'the other'. For those who participated, the war gave meaning to their existence, turning war into an existential experience and not an instrumental one.[31]

The horrific attacks of 9/11 inspired a wealth of studies on the apparent new form of catastrophic terrorism, on radicalization processes, the logic of suicide bombings and the role of religion.[32] Here, too, studies on Al-Qaeda, the Taliban, Hezbollah and more recently IS show that the Western instrumental perspective on war may partly explain the behaviour of such groups, but also that it is a limited and culturally determined one. The 9/11 attacks, Jurgensmeyer concluded, were the manifestation of an everlasting 'cosmic' metaphysical and existential religious battle, or so the perpetrators of the attacks experienced it.[33]

The Second Lebanon War of 2006, a rude awakening for Israel, also showed the limitations of the traditional categorization of types of wars used by Western academics and military personnel. Hezbollah, a terrorist movement, now featured an arsenal of medium to long range missiles, weapons traditionally not associated with terrorist organizations, and applied tactics of different types of warfare: standard guerrilla tactics but also positional defence of villages, whereby Hezbollah managed to take out Israeli tanks. This mix of terrorist tactics, guerrilla type actions and regular army operations, combined with a sophisticated media organization, inspired Frank Hoffman to call it Hybrid Conflict, drawing attention to this category-breaking aspect.[34]

Strategic narratives and so-called 'Virtual War' – the use of internet and social media – had now become an obvious key front. Hezbollah claimed victory over Israel, not because of military success, but through a targeted media campaign. Elsewhere groups such as the Al-Qaeda, Taliban and IS also boosted the perception of their power through showing social media images of suicide bombers, horrific killings and ambushes on Western troop

patrols, all of which were carried out, not because of their immediate tactical military effects, but rather to produce propaganda material.[35] By promoting sensational media images, terrorist groups capitalized on the 'power of failure': even if attacks missed their primary target they proved they still existed and the government was failing in its counter-terrorist strategy. In response, a flurry of studies and new doctrines suggested counters to such narratives or ways to employ them proactively.[36]

Right from the start of the mission in Afghanistan there was an intense discussion about the validity of the liberal statebuilding model and its strategic value, with most analysts agreeing that its core assumptions were flawed and building local institutions and bodies that have local legitimacy should take priority, even if they are based on norms and values that are diametrically opposed to those of the West.[37] Meanwhile, in response to the strategic and operational problems in Iraq and Afghanistan, classical works on counterinsurgencies were reviewed for their current relevance. Traditional concepts such as hearts and minds campaigns, and clear-hold-build were rediscovered, but also criticized as contemporary insurgencies differed greatly from the groups on which the classical COIN theorists based their work. Insurgents are no longer necessarily intent on taking over the state and no longer was there a dichotomy of a state against one insurgent. Instead, insurgent and terrorist movements are not monolithic organizations and within such movements several groups may compete with one another.[38]

The problems with counterinsurgency inspired studies into alternatives that could offer a 'low footprint-low risk' solution. Counterinsurgency, like statebuilding, is personnel-intensive, requires long-term commitment and is highly dependent on the quality and legitimacy of the host nation's government. Moreover, it potentially leads to a significant number of casualties among Western military personnel and they are rarely successful.[39] The success of Operation Enduring Freedom in 2001 in which the Taliban was ousted by the combination of special forces, air power and local rebels, or proxies, brought proxy warfare into the spotlight. This model has since also been used successfully applied against Gaddafi in 2011 and IS in Iraq yet also critically reviewed as it leaves the fight to the proxy and success depends on to what extent and for how long the interests, objectives, stamina and risk assessments of the Western coalition match those of the proxy forces.[40]

A second alternative was presented by armed Unmanned Aerial Vehicles (UAVs). Drones allow prolonged surveillance of members of terror movements and insurgents and engage them in so-called targeted killing actions. Beyond the immediate destructive effects, this may also serve as a deterrent. However, fierce critique argued this practice constituted illegitimate 'extra-judicial killing' and would lead to the casual use of force because it entailed few risks politically. Moreover, a PlayStation mentality was expected: a drone attack might look like a video game for young drone pilots. War then becomes surreal and moral disengagement and dehumanization

occur, explaining, according to critics, the apparently large number of civilian casualties. Subsequent empirical studies demonstrated that many of the initial concerns and criticisms were unjustified. The Red Cross even concluded that carefully deployed drones made it possible in principle to better follow the rules of humanitarian war law than with manned aircraft.[41]

Finally, Cyberwarfare. This became a dominant topic after the Russian cyberattack on Estonia in 2007, the increasing Chinese cyber activity and the Stuxnet attack on Iran in 2012. Early studies contrasted cyberattack characteristics with those of traditional kinetic attacks with high tech weapons, suggesting cyber weapons are available to all kinds of non-state actors; they are most likely 'one-shot' weapons (once used, a defence will be developed quickly) and that effects of cyberattacks are transient. Whether cyberattacks can have strategic effects and whether they can play a role as a deterrent are an ongoing debate. At the same time, cyber warfare will lead to a substantial power shift and a potential threat to the international legal order (see also Chapters 13 and 14).[42] Another strand of inquiry questioned to what extent the existing framework of international and humanitarian law of war is sufficient for cyber warfare, while Thomas Rid challenged whether cyberattacks can be considered war in the Clausewitzian sense at all.

Understanding the paradox of strategic underperformance

There is a remarkable paradox: on the one hand problems that can partly be traced back to lacunae in the strategic frame of reference, while on the other hand a parallel blossoming of the study of war producing strategically relevant insights that could and perhaps should have been a source of influence during policy and strategy developments at the time. This paradox has an almost trivial explanation. Thorough academic work takes time and is therefore inevitably reactive. It took several years to rediscover and update knowledge about coercive diplomacy. Revision of peacekeeping doctrines also took years, including the trauma of Srebrenica and Rwanda and the subsequent crisis in UN peacekeeping operations, in which the West was reluctant to set up or participate in UN operations. It also takes a long time for these kinds of new insights to be incorporated into military doctrines, UN manuals, new curricula in university education programs and military courses. It then remains to be seen whether such knowledge can also influence a strategic decision-making process in time.

Studies on institutionalization processes, learning processes and military innovation also suggest that the dissemination and embedding of new insights, doctrines and practices does not always proceed quickly in armed forces, with their strong identity and organizational culture, and their inherent conservative nature regarding ideas that may not yet have demonstrated their merits in practice.[43] Moreover, narrow organizational interests and inter-service rivalry, service-specific ongoing investment programs and national political priorities can all act as a filter, downplaying analyses and

lessons learned that are perhaps not irrelevant but not in the interest from a specific service's perspective which is in the middle of a fight for shrinking budgets. Moreover, it can be argued that the most recent war is a unique and one-off case (the fallacy of the significant exception), or that a particular case will not often reoccur for a particular country. Analyses are thus politicized.[44]

Furthermore, during operations deployed units were forced to engage in continuous and rapid adaptation processes to respond to the tactical situation on the ground which invariably proved different from the initial military and political assessments. This could result in new tactics, rapid introduction of new equipment or requests to adjust Rules of Engagement.[45] Units passed on painful experiences, often through informal learning and communication processes. In a force with institutional lessons learned processes and associated organizations such as in the United States (and to some extent also in the United Kingdom), this resulted, with some delay, in excellent new doctrines.[46] However, understandably, in the context of ongoing tensions among defence organizations, the institutionalization – internalization – of lessons learned in units has often been problematic, or has been neglected, certainly if no formalized learning processes existed, which was the case in most European armed forces.[47]

An additional factor has been the fluidity of defence policy and the subsequent rapid pace of change that the armed forces have had to respond to since 1990. The geopolitical scope of their efforts and the variety of mission types only increased. From fully educated in, trained and equipped for Air-Land Battle, Follow-on-Forces-Attack and joint warfare in which infantry, armour, artillery and fighter aircraft would coordinate to combat the Red Enemy, to the unarmed Blue Helmet UN missions to keep peace that was not there. From the German plains to African zones of turmoil to alleviate humanitarian needs, from the Atlantic to intercept Russian submarines to combat piracy in the Indian Ocean, to Afghanistan to rebuild the country and suppress a vicious insurgency. And, having just returned from Afghanistan and the skies over Libya and Iraq, it turned out that units had to prepare again for large-scale warfare, including nuclear deterrence. This is just a sampling of the high tempo and scope of strategic and operational changes that Western armed forces have faced, amid ongoing austerity, force reductions, the closure of barracks, headquarters and air bases. After one type of mission or conflict a different type of mission demanded the attention of the same units, with the other type requiring substantially different expertise. That happened in 1990, in 2001 and reoccurred in 2014: now the demand for expertise, training and exercise for COIN missions with a focus on a comprehensive and population centric approach, and non-kinetic influence methods, is less pressing for most European armed forces than regaining expertise in waging large-scale enemy-centric combat.

This has a direct influence on the question which knowledge and expertise will be institutionalized and updated. Moreover, many European member

states do not have a national operational headquarter where military strategy is developed; that theme has de facto mostly been delegated to NATO. In various countries there is also no intensive contact between the theoretical academic world, the ministries of defence and foreign affairs and the 'operators' within the armed forces. And sometimes, Elliott noticed, those communities talk in different languages; they are separate epistemological communities.[48] While these differences are to be expected, the danger lurks of institutional isolationism and institutional amnesia is then to be expected: every organization views the strategic problems from its own limited perspective and from its own organization-specific rationality.

The shadow of the past

While in light of these factors criticism of Western politicians and military commanders must be nuanced, the costly insights and traumas of the three decades of war should not go unheeded as they aided our understanding of contemporary war. Whereas up to 2014, it could be argued that real security risks were far away, Europe, and the West is once again confronted with and surprised by tragic security policy developments nearby: strategic competition, an assertive Russia, the rise of nationalist, right-wing extremist groups and authoritarian governments, all of which risk undermining cohesion within the EU and NATO. At the same time, there is little to suggest that the situation in the Arc of Instability will change substantially and positively in the coming years.[49] In that sense the three decades of war offer sufficient information to provide a plausible image of the future Westerns governments and their militaries should be prepared for.[50] The future is less uncertain than generally believed to be, or, as Nicholas Taleb stated provocatively, the future is here, the most important parts of it were made long ago.[51] It suggests that the variety of types of war and modes of warfare encountered during the past 30 years and captured in the following five images will probably offer a minimum baseline for thinking about the conduct of war in the next decade.

One dominant school of thought sees continuity with wars revolving around vicious actions of violent non-state actors such as IS and criminal organizations, while the distinction between the type of actor is actually meaningless. Sometimes ethnicity or religion is a driver for the struggle, but often it goes hand in hand with the pursuit of economic profit. Their battlefield is increasingly the city, an environment in which it is difficult for Western soldiers to operate.[52] There will be 'durable disorder'. This harps back to van Creveld's 1989 book *The Transformation of War,* Kaldor's New Wars thesis from the 1990s and Hoffman's Hybrid Conflict concept from 2007. According to McFate, these groups will increasingly be able to inflict damage upon Western countries via cyberattacks, corruption and the use of drones.[53] They can easily organize themselves into 'smart mobs' via social media. With their barbaric tactics, they will be able to intimidate

populations, echoing past visions of the future that warn of expanding anarchism in much of the world.[54]

Mary Kaldor argued, in light of the above, that Western states must be prepared for intra-state wars, humanitarian crises and corresponding humanitarian operations. Indeed, most analysts expect humanitarian crises to increase in number. Coining this image the 'liberal peace security culture', she associates it with effective international organizations such as the OSCE, the EU and the UN. Continuing on the laudable ideals of the 1990s and the concept of Human Security, this cosmopolitan vision sees a future in which wars in failing and fragile states must be resolved and violence curtailed through peacekeeping operations to alleviate humanitarian suffering. To this end, Western armed forces must act *de facto* as cosmopolitan police units that provide security and stability in villages in order to create space in which to start a peaceful political process.

The third image disagrees with Kaldor, arguing that the future, like the past, is irregular, and militaries will deploy predominantly in a counter-insurgency role, in a multitude of protracted conflicts in unstable regions, using mainly special forces, training of proxy forces, sophisticated surveillance systems capable of long-term observation of areas and armed drones if necessary to perform a precision strike on a few individuals.[55] The ambition is not so much to defeat the insurgents or terrorist movements as to curb the risks these groups can present for increasing regional destabilization and/or as a direct threat to Western societies. In that it continues on the Global War on Terror, the so-called Long War, and US operations ongoing in several African countries as well as against IS.[56] 'Surrogate Warfare', according to Krieg and Rickli: the West tries to exert influence with high technology and minimal physical presence and therefore political risk in conflict areas.[57] War as risk management indeed, and certainly immaculate.

The fourth image concerns the renewed geopolitical rivalry between the United States (with Europe at hand), Russia and China. The concept of hybrid threats has recently been supplemented with terms such as 'new total warfare', 'political warfare' and 'gray zone warfare'.[58] All of these suggest that strategic competition should be viewed as war, in the sense that, just as during the Cold War, strategy concerns a wide range of instruments and activities in various military and especially non-military domains, and second, that in the application of those instruments it can affect various sections of Western societies. Defence requires a so-called whole of society approach to guard against continuous use of non-kinetic actions intent to exert influence such as economic espionage through cyberattacks, economic sanctions and financial warfare, bribery and intimidation of politicians (and liquidation through poisoning if necessary), and financing of militant anti-European political groups in democratic states and even providing these groups with weapons.[59] But it is also about gaining influence through 'cool' social media, including the distribution of fake news.[60] Hackers, troll armies, tech companies, media organizations, banks, research centres, academic

institutions and energy suppliers all are actors in this strategic competition. War and peace, concepts categorically distinguished in the West, overlap.[61]

Finally, contradicting John Mueller, echoing the events since 2014, various authors see a return of large-scale conflict in addition to the 'Cool War' just outlined. War in the classical sense, like an armed conflict between two large countries, is no longer considered impossible and less improbable than, for example, in 1999. The damping effect of international institutions is steadily diminishing and the need for authoritarian regimes to pursue aggressive foreign policies for national purposes is increasing, as is their capacity for offensive actions. Small-scale 'probes' are expected which will not justify a collective armed response from the West, yet slowly aim to change the status quo and undermine the power position of the West (especially the United States) and test the willingness to commit to serious reprisals. New technologies will be used such as hypersonic missiles, swarms of drones and killer robots. AI will analyse large amounts of data from large numbers of networked commercial and military sensors and satellites.[62] All enhance the risk of escalation.[63] This vision reflects the ongoing shift in the balance of power, something the COVID-19 crisis is expected to accelerate, with a declining influence of the United States, and thus of the West. The liberal world order is subject to erosion and liberal Western ideas are under discussion, in both non-Western and various Western countries.[64] This is not a return to the Cold War, because unlike that period, actors are now actively seeking to disrupt stability. We will enter an interregnum in which ideology will once again play an important role. Fukuyama has been discredited: there is in fact a competitor for Western liberalism: authoritarianism. The question is which international order will win this competition.[65]

Conclusion: strategic history and the multiple faces of war

Like the past, the future of war is plural and defence policy based on just one particular future scenario is irresponsible.[66] As Clausewitz famously argued, war is a many-headed and changeable phenomenon, like a chameleon. In retrospect the West has, arguably, not taken this to heart sufficiently. Not all futures are equally relevant for all countries of course. The future of war looks partly different for the Europeans than for the United States. Yet, if strategic surveys combined with what we know of the past three decades may serve as guidepost, for many Western states the strategic panorama holds a future in which they will continue to be forced to act in a context of sophisticated barbarism, launching peacekeeping operations to resolve humanitarian emergencies, and do so while limiting political risk as much as possible by relying partly on proxies. At the same time, it will have to be alert and proactive in the context of the Cool War, which is part of a strategic competition that also takes place on European territory which also demands taking seriously again the risk of major war and to enhance conventional and nuclear deterrence credibility.

War must regrettably be put back into the Western societal discourse, not to casually consider it as a normal feature of international affairs and wage it with a degree of indifference, but to regain the frame of reference so that we can understand this tragic phenomenon in all its facets and deploy the military instrument strategically, if necessary. Perhaps the intellectual father of War Studies, Sir Michael Howard, was right when he wrote in 2000 that war is the norm while peace is a recent fragile invention and a historical exception.[67] War, alas, like in the past, has a bright future.

Notes

1 Alex Bellamy and Paul Williams, *Understanding Peacekeeping*, 2nd edition (Cambridge: Polity Press, 2010), 13–41.
2 Peter Viggo Jakobsen, 'The Yugoslav Wars', in Peter Viggo Jakobsen, ed., *Western Use of Coercive Diplomacy after the Cold War* (London: Palgrave, 1998), 70–109.
3 Thierry Tardy, 'United Nations Protection Force (UNPROFOR—Bosnia and Herzegovina)', in Joachim Koops, et al., eds., *The Oxford Handbook of United Nations Peacekeeping Operations* (Oxford: Oxford University Press, 2015), 371–394.
4 See Benjamin Lambeth, *NATO's Air War for Kosovo* (Santa Monica, CA: RAND, 2001), Ivo Daalder and Michael O'Hanlon, *Winning Ugly, NATO's War to Save Kosovo* (Washington, DC: Brookings, 2000).
5 Frans Osinga, 'De Strategische Pauze Voorbij: Veiligheid, Defensie en de Westerse krijgsmacht na 9/11', *Militaire Spectator* 180:9 (2011), 398–415.
6 Francis Fukuyama, 'The Imperative of State-building', *Journal of Democracy* 15:2 (2004), 17–31, Mats Berdal and Dominik Zaum, *Political Economy of Statebuilding* (Abingdon: Routledge, 2013).
7 Ben Barry, *Harsh Lessons, Iraq, Afghanistan and the Changing Character of War* (London: IISS, 2016).
8 AIV, *Instabiliteit Rond Europa, Confrontatie met een Nieuwe Werkelijkheid, Rapport* 94 (The Hague: AIV, 2015).
9 Matthew Kroenig, 'Facing Reality: Getting NATO Ready for a New Cold War', *Survival* 57:1 (2015), 49–70, Alexander Lanoszka, 'Russian Hybrid Warfare and Extended Deterrence in Eastern Europe', *International Affairs* 92:1 (2016), 175–195.
10 Dmitry (Dima) Adamsky, 'From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture', *Journal of Strategic Studies* 41:1–2 (2018), 1–25, Stephan Frühling and Guillaume Lasconjarias, 'NATO, A2/AD and the Kaliningrad Challenge', *Survival* 58:2 (2016), 95–116.
11 Charles Moskos, John Allan Williams, and David Segal, eds., *The Postmodern Military, Armed Forces after the Cold War* (Oxford: Oxford University Press, 2000), Mike Bourne, 'War and Killing', in Mike Bourne, ed., *Understanding Security* (New York: Palgrave, 2014), 136–157.
12 Mary Kaldor, *New and Old Wars* (Cambridge: Polity, 1999), Adrian Hyde-Price, 'European Security, Strategic Culture, and the Use of Force', *European Security* 13:4 (2004), 323–343.
13 J. Mueller, *Retreat from Doomesday: The Obsolescence of Major War* (New York: Basic Books, 1989), Robert Kagan, *Of Paradise and Power: America and Europe in the New World Order* (New York: Knopf, 2003).
14 Christopher Coker, *Humane Warfare* (Abingdon: Routledge, 2001), 1–23, Patrick Mello, 'National Restrictions in Multinational Military Operations: A Conceptual Framework', *Contemporary Security Policy* 40:1 (2019), 38–55.

15 I.G.B.M. Duyvesteyn, *Strategisch analfabetisme. De kunst van strategisch denken in moderne militaire operaties* (Leiden University, Inaugural Lecture, 2013); H. Amersfoort, 'Nederland, de weg kwijt. Over de teloorgang van de militaire strategie en de noodzaak van geschiedenis', *Militaire Spectator* 185:5 (2016), 217–231, M.W.M. Kitzen and F.H. Thönissen, 'Strategische vaagheid, Hoe het gebrek aan strategische visie het lerend vermogen van de Koninklijke Landmacht beperkt', *Militaire Spectator* 187:4 (2018), 206–223.
16 Carl Rochelle, 'NATO Grapples with "War by Committee"', *CNN*, 19 April 1999.
17 Christopher Elliott, *High Command: British Military Leadership in the Iraq and Afghanistan Wars* (London: Hurst, 2015), Hew Strachan, *The Direction of War* (Cambridge: Cambridge University Press, 2013).
18 Hew Strachan, 'The Lost Meaning of Strategy', *Survival* 47:3 (2005), 33–54.
19 Cedric de Coning and Karsten Friis, 'Coherence and Coordination: The Limits of the Comprehensive Approach', *Journal of International Peacekeeping* 15:1–2 (2011), 243–272.
20 Rupert Smith and Ilana Bet-El, *The Utility of Force, The Art of War in the Modern World* (New York: Knopf, 2005).
21 Stephen Downes-Martin, 'Operations Assessment in Afghanistan Is Broken, What Is to be Done?' *Naval War College Review*, 64:4 (2011), 103–325.
22 See Patricia Weitsman, *Waging War, Alliances, Coalitions and Institutions of Interstate Violence* (Stanford, CA: Stanford University Press, 2014), US General Accounting Office, *Kosovo Air Operations: Need to Maintain Alliance Cohesion Resulted in Doctrinal Departures* (Washington, DC: US General Accounting Office, 2001).
23 Christopher Paul, *Counterinsurgency Scorecard, Afghanistan* (Santa Monica, CA: RAND, 2011), Seth Jones, *In the Graveyard of Empires: America's War in Afghanistan* (New York: W. W. Norton & Company, 2010).
24 Theo Farrell, *Unwinnable, Britain's War in Afghanistan 2001–2014* (London: The Bodley Head, 2017).
25 Mats Berdal, 'A Mission Too Far? NATO and Afghanistan, 2001–2014', in Daniel Marston and Tamara Leary, eds., *War, Strategy and History, Essays in Honour of Professor Robert O'Neill* (Canberra: ANU Press, 2016), 155–178.
26 For a summary of those studies and the various arguments in the debate, see Keith Shimko, *The Iraq Wars and America's Military Revolution* (Cambridge: Cambridge University Press, 2010).
27 T.V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers* (Cambridge: Cambridge University Press, 1994), Peter Viggo Jakobsen, *Western Use of Coercive Diplomacy after the Cold War* (London: Macmillan, 1998), Daniel Byman, and Matthew Waxman, *The Dynamics of Coercion* (Cambridge: Cambridge University Press, 2002).
28 Frans Osinga, 'The Rise of Transformation', in Terry Terriff, Frans Osinga and Theo Farrell, eds., *A Transformation Gap? American Innovations and European Military Change* (Stanford, CA: Stanford University Press, 2010), 14–34.
29 Mats Berdal, 'Lessons Not Learned: The Use of Force in 'Peace Operations in the 1990s', *International Peacekeeping* 7:4 (2000), 55–74.
30 Virginia Page Fortna, 'Does Peacekeeping Keep Peace?', *International Studies Quarterly* 48:2 (2004), 269–292, Monica Duffy Toft, 'Ending Civil Wars, A Case for Rebel Victory?', *International Security* 34:4 (2010), 7–38, Roland Paris, 'The 'Responsibility to Protect' and the Structural Problems of Preventive Humanitarian Intervention', *International Peacekeeping* 21:5 (2014), 569–603.
31 Martin van Creveld, *The Transformation of War* (New York: The Free Press, 1991), Kaldor, *New and Old Wars*, Richard Shultz and Andrea Dew, *Insurgents, Terrorists and Militia's, The Warriors in Contemporary Conflict* (New York: Columbia University Press, 2006), Stuart Kaufman, 'Symbolic Politics or Rational

Choice? Testing Theories of Extreme Ethnic Violence', *International Security* 30:4 (2006), 45–86, Richard Jackson and Helen Dexter, 'The Social Construction of Organized Political Violence: An Analytical Framework', *Civil Wars*, 16:1, 1–23, Chris Hedges, *War Is a Force That Gives Us Meaning* (New York: Public Affairs, 2002).

32 Mark Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

33 Mark Juergensmeyer, *Terror in the Mind of God* (Berkeley: University of California Press, 2003).

34 David Johnson, *Hard Fighting: Israel in Lebanon and Gaza* (Santa Monica, CA: RAND, 2006), Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: The Potomac Institute of Policy Studies Arlington, Virginia, 2007).

35 David Betz, 'The Virtual Dimension of Contemporary Insurgency and Counter-insurgency', *Small Wars & Insurgencies* 19:4 (2008), 510–540, Thomas Rid, and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westport, CT: Praeger, 2009), James P. Farwell, 'Jihadi Video in the "War of Ideas"', *Survival* 52:6 (2010), 127–150, Jens Ringsmose and Berit Kaja Børgesen, 'Shaping Public Attitudes towards the Deployment of Military Power: NATO, Afghanistan and the Use of Strategic Narratives', *European Security* 20:4 (2010), 505–528.

36 Eric V. Larson, et al., *Foundations of Effective Influence Operations* (Santa Monica, CA: RAND, 2009), US Joint Forces Command, *Commander's Handbook for Strategic Communication and Communication Strategy* (Suffolk, VA: US Joint Forces Command, 2010), Kurt Braddock and John Horgan, 'Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism', *Studies in Conflict & Terrorism* 39:5 (2–16), 381–404.

37 Roland Paris and Timothy Sisk, *The Dilemmas of Statebuilding* (London: Routledge, 2009), Nicolas Lemay-Hébert, 'Statebuilding without Nation-Building? Legitimacy, State Failure and the Limits of the Institutionalist Approach', *Journal of Intervention and Statebuilding* 3:1 (2009), 21–45, Roger Mac Ginty and Oliver P. Richmond, 'The Local Turn in Peace Building: A Critical Agenda for Peace', *Third World Quarterly* 34:5 (2013), 763–783.

38 David Kilcullen, *The Accidental Guerrilla* (Oxford: Oxford University Press, 2009), Frank Hoffman, 'Neo-Classical Counterinsurgency?', *Parameters* 37:2 (2007), 71–87, Christopher Paul, Colin P. Clarke, Beth Grill, and Molly Dunigan, *Paths to Victory: Lessons from Modern Insurgencies* (Santa Monica, CA: RAND, 2013), Douglas Porch, *Counterinsurgency: Exposing the Myths of the New Way of War* (Cambridge: Cambridge University Press, 2013).

39 Gil, Merom, *How Democracies Lose Small Wars* (New York: Cambridge University Press, 2003).

40 Richard Andres Craig Wills, and Thomas E. Griffith, Jr., 'Winning with Allies: The Strategic Value of the Afghan Model', *International Security* 30:3 (2005/2006), 124–160, Joseph L. Votel and Eero R. Keravuori, 'The By-With-Through Operational Approach', *Joint Force Quarterly* 89:2 (2018), 40–47, Andrew Mumford, *Proxy Warfare* (Cambridge: Polity Press, 2013).

41 See for a summary Frans Osinga, 'Bounding the Debate on Drone Warfare', in Herman Amersfoort et al., eds., *Moral Responsibility & Military Effectiveness* (The Hague: Asser, 2013), 243–278.

42 Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013), Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), Erik Gartzke, 'The Myth of Cyberwar, Bringing War in Cyberspace Back Down to Earth', *International Security* 38:2 (2013), 41–73, Lucas Kello, *The Virtual Weapon and International Order* (Hartford, CT: Yale University Press, 2017), Michael P. Fischerkeller and Richard J. Harknett, 'Deterrence

is Not a Credible Strategy for Cyberspace', *Orbis* 61:3 (2017), 381–393, P.A.L. Ducheine, 'Military Cyber Operations', in T. D. Gill and D. Fleck, eds., *The Handbook of the International Law of Military Operations, 2nd edition* (Oxford: Oxford University Press, 2015), 456–475.

43 See Tom Dyson, *Organisational Learning and the Modern Army* (Abingdon: Routledge, 2020).

44 Adam Grissom, 'The Future of Military Innovation Studies', *Journal of Strategic Studies* 29:5 (2006), 905–934, Andrew Hill and Stephen Gerras, 'Systems of Denial, Strategic Resistance to Military Innovation', *Naval War College Review* 69:1 (2016), 109–132.

45 Sergio Catignani, '"Getting COIN" at the Tactical Level in Afghanistan: Reassessing Counter-Insurgency Adaptation in the British Army', *Journal of Strategic Studies* 35:4 (2012), 1–27, Brian Burton and John Nagl, 'Learning As We Go: The US Army Adapts to Counterinsurgency in Iraq, July 2004–December 2006', *Small Wars and Insurgencies* 19:3 (2008), 303–327, Frans Osinga, Theo Farrell, and James Russell, eds., *Military Adaptation and the War in Afghanistan* (Stanford, CA: Stanford University Press, 2013).

46 For instance, US Army: *Field Manual 3-24 Counterinsurgency* (Washington, DC: Headquarters of the Department of the Army, 2006), Development, Concepts, and Doctrine Center (DCDC), *UK Joint Doctrine Publication 3-40, Security and Stabilisation: The Military Contribution* (Shrivenham: DCDC, 2009).

47 See the various country studies in Terriff, Osinga, and Farrell, *A Transformation Gap*?

48 Elliot, *High Command*.

49 See DCDC, *British Global Strategic Trends – Out to 2045*, 6th edition (Shrivenham, DCDC, 2018), National Intelligence Council, *Global Trends Report, Paradox of Progress* (Washington, DC: National Intelligence Council, 2017).

50 For a critical discussion of the many and diverging visions of future war, see Lawrence Freedman, *The Future of War, A History* (New York: Public Affairs, 2017).

51 See for studies on the role of uncertainty Stephan Frühling, 'Uncertainty, Forecasting and the Difficulty of Strategy', *Comparative Strategy* 25:1 (2006), 19–31, Patrick Porter, 'Taking Uncertainty Seriously: Classical Realism and National Security', *European Journal of International Security* 1:2, 239–260, Nassim Nicholas Taleb, *Antifragile Things that Gain from Disorder* (New York: Random House, 2014).

52 David Kilcullen, *Out of the Mountains, the Coming Age of the Urban Guerrilla* (London: Hurst, 2013).

53 Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder* (New York: William Morrow, 2019).

54 See Robert Kaplan, *The Coming Anarchy: Shattering the Dreams of the Post Cold War* (New York: Vintage Books, 2001), Aaron Wildavsky, *The Real World Order: Zones of Peace/Zones of Turmoil* (Chatham: Chatham House, 1993).

55 Seth Jones, *Waging Insurgent Warfare, Lessons from the Vietcong to the Islamic State* (Oxford: Oxford University Press, 2016), Seth Jones, 'The Future of Warfare Is Irregular', *The National Interest*, 26 August 2018, https://nationalinterest.org/feature/future-warfare-irregular-29672.

56 Daniel Byman, 'Why States Are Turning to Proxy War', *The National Interest*, 26 August 2018, https://nationalinterest.org/feature/why-states-are-turning-proxy-war-29677.

57 Andreas Krieg and Jean-Marc Rickli, 'Surrogate Warfare: The Art of War in the 21st Century?' *Defence Studies* 18:2 (2018), 113–130.

58 Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Stockholm: Swedish Defence University, 2018), Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare:*

Russia, The West, and the Coming Age of Global Digital Competition (Washington, DC: Brookings Institute, 2017).

59 Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND, 2018).

60 David Rothkopf, 'The Cool War', *Foreign Policy*, 20 February 2013, Noah Feldman, *Cool War: The Future of Global Competition* (New York: Random House, 2013), Michael Gross and Tamar Meisels, eds., *Soft War, the Ethics of Unarmed Conflict* (Cambridge: Cambridge University Press, 2017), Peter Singer, *LikeWar, the Weaponization of Social Media* (Boston, MA: Eamon Dolan, 2018).

61 Sean Monaghan, ed., *Countering Hybrid Warfare* (Shrivenham: DCDC, 2018), Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, *Gaining Competitive Advantage in the Gray Zone, Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND, 2019), Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *Modern Political Warfare, Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018).

62 Keneth Payne, *Strategy, Evolution and War, From Apes to Artificial Intelligence* (Washington, DC: Georgetown University Press, 2018), Christian Brose, 'The New Revolution in Military Affairs, War's New Sci-Fi Future', *Foreign Affairs* 98:3 (2019), 122–134, Robert Latiffe, *Future War, Preparing for the New Global Battlefield* (New York: Vintage Books, 2017).

63 Michael Mandelbaum, *The Rise and Fall of Peace on Earth* (New York: Oxford University Press, 2019), Jesse T. Wasson, and Christopher E. Bluesteen, 'Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems', *Defence Studies* 18:4 (2018), 433–453, Rupal Mehta, 'Extended Deterrence and Assurance in an Emerging Technology Environment', *Journal of Strategic Studies* (2019).

64 Richard Haass, 'How a World Order Ends: And What Comes in Its Wake', *Foreign Affairs* 98:1 (2019), 22–30, Alina Polyakova and Benjamin Haddad, 'Europe Alone, What Comes after the Transatlantic Alliance', *Foreign Affairs* 98:4 (2019), 109–120.

65 Jack Snyder, 'The Broken Bargain, How Nationalism Came Back', *Foreign Affairs* 98:2 (2019), 54–60, Cas Mudde, 'Europe's Populist Surge, A Long Time in the Making', *Foreign Affairs* 95:6 (2016), 25–30, Hal Brands, 'Democracy vs Authoritarianism: How Ideology Shapes Great-Power Conflict', *Survival* 60:5 (2018), 61–114.

66 Frank Hoffman, 'The Future Is Plural, Multiple Futures for Tomorrow's Joint Force', *Joint Force Quarterly* 88:1 (2018), 4–13, Robert A. Johnson, 'Predicting Future War', *Parameters* 44:1 (2014), 65–76.

67 Michael Howard, *The Invention of Peace* (Hartford, CT: Yale University Press, 2000).

References

Adamsky, Dmitry (Dima), 'From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture', *Journal of Strategic Studies* 41:1–2 (2018), 1–25.

AIV, *Instabiliteit Rond Europa, Confrontatie met een Nieuwe Werkelijkheid, Rapport* 94 (The Hague: AIV, 2015).

Amersfoort, H., 'Nederland, de weg kwijt. Over de teloorgang van de militaire strategie en de noodzaak van geschiedenis', *Militaire Spectator* 185:5 (2016), 217–231.

Andres, Richard, Wills, Craig, and Griffith, Thomas E. Jr., 'Winning with Allies: The Strategic Value of the Afghan Model', *International Security* 30:3 (2005/2006), 124–160.

Bellamy, Alex, and Williams, Paul, *Understanding Peacekeeping*, 2nd edition (Cambridge: Polity Press, 2010).

Ben Barry, *Harsh Lessons, Iraq, Afghanistan and the Changing Character of War* (London: IISS, 2016).

Benjamin, Lambeth, *NATO's Air War for Kosovo* (Santa Monica, CA: RAND, 2001).

Berdal, Mats, 'A Mission Too Far? NATO and Afghanistan, 2001–2014', in *War, Strategy and History, Essays in Honour of Professor Robert O'Neill*, Daniel Marston and Tamara Leary, eds., 155–178 (Canberra: ANU Press, 2016).

Berdal, Mats, 'Lessons Not Learned: The Use of Force in "Peace Operations in the 1990s"', *International Peacekeeping* 7:4 (2000), 55–74.

Berdal, Mats and Zaum, Dominik, *Political Economy of Statebuilding* (Abingdon: Routledge, 2013).

Betz, David, 'The Virtual Dimension of Contemporary Insurgency and Counterinsurgency', *Small Wars & Insurgencies* 19:4 (2008), 510–540.

Bourne, Mike, 'War and Killing', in *Understanding Security*, Mike Bourne, ed., 136–157 (New York: Palgrave, 2014).

Braddock, Kurt and Horgan, John, 'Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism', *Studies in Conflict & Terrorism* 39:5 (2–16), 381–404.

Brands, Hal, 'Democracy vs Authoritarianism: How Ideology Shapes Great-Power Conflict', *Survival* 60:5 (2018), 61–114.

Brose, Christian, 'The New Revolution in Military Affairs, War's New Sci-Fi Future', *Foreign Affairs* 98:3 (2019), 122–134.

Burton, Brian and Nagl, John, 'Learning as We Go: the US Army Adapts to Counterinsurgency in Iraq, July 2004–December 2006', *Small Wars and Insurgencies* 19:3 (2008), 303–327.

Byman, Daniel, 'Why States Are Turning to Proxy War', *The National Interest*, 26 August 2018, at https://nationalinterest.org/feature/why-states-are-turning-proxy-war-29677.

Byman, Daniel and Waxman, Matthew, *The Dynamics of Coercion* (Cambridge: Cambridge University Press, 2002).

Catignani, Sergio, '"Getting COIN" at the Tactical Level in Afghanistan: Reassessing Counter-Insurgency Adaptation in the British Army', *Journal of Strategic Studies* 35:4 (2012), 1–27.

Coker, Christopher, *Humane Warfare* (Abingdon: Routledge, 2001).

Coning, Cedric de, and Friis, Karsten, 'Coherence and Coordination: The Limits of the Comprehensive Approach', *Journal of International Peacekeeping* 15:1–2 (2011), 243–272.

Creveld, Martin van, *The Transformation of War* (New York: The Free Press, 1991).

Daalder, Ivo and O'Hanlon, Michael, *Winning Ugly, NATO's War to Save Kosovo* (Washington, DC: Brookings, 2000).

DCDC, *British Global Strategic Trends – Out to 2045*, 6th edition (Shrivenham: DCDC, 2018).

Development, Concepts, and Doctrine Center (DCDC), *UK Joint Doctrine Publication 3–40, Security and Stabilisation: The Military Contribution* (Shrivenham: DCDC, 2009).

Downes-Martin, Stephen, 'Operations Assessment in Afghanistan Is Broken, What Is to be Done?' *Naval War College Review*, 64:4 (2011), 103–325.

Ducheine, P.A.L., 'Military Cyber Operations', in *The Handbook of the International Law of Military Operations, 2nd edition*, T. D. Gill and D. Fleck, eds., 456–475 (Oxford: Oxford University Press, 2015).
Duyvesteyn, I.G.B.M., *Strategisch analfabetisme. De kunst van strategisch denken in moderne militaire operaties* (Leiden University, Inaugural Lecture, 2013).
Dyson, Tom, *Organisational Learning and the Modern Army* (Abingdon: Routledge, 2020).
Elliott, Christopher, *High Command: British Military Leadership in the Iraq and Afghanistan Wars* (London: Hurst, 2015).
Farrell, Theo, *Unwinnable, Britain's War in Afghanistan 2001–2014* (London: The Bodley Head, 2017).
Farwell, James P., 'Jihadi Video in the 'War of Ideas', *Survival* 52:6 (2010), 127–150.
Feldman, Noah, *Cool War: The Future of Global Competition* (New York: Random House, 2013).
Fischerkeller, Michael P., and Harknett, Richard J., 'Deterrence Is Not a Credible Strategy for Cyberspace', *Orbis* 61:3 (2017), 381–393.
Fortna, Virginia Page, 'Does Peacekeeping Keep Peace?' *International Studies Quarterly* 48:2 (2004), 269–292.
Freedman, Lawrence, *The Future of War, A History* (New York: Public Affairs, 2017).
Frühling, Stephan, 'Uncertainty, Forecasting and the Difficulty of Strategy', *Comparative Strategy* 25:1 (2006), 19–31.
Frühling, Stephan, and Lasconjarias, Guillaume, 'NATO, A2/AD and the Kaliningrad Challenge', *Survival* 58:2 (2016), 95–116.
Fukuyama, Francis, 'The Imperative of State-Building', *Journal of Democracy* 15:2 (2004), 17–31.
Gartzke, Erik, 'The Myth of Cyberwar, Bringing War in Cyberspace Back Down to Earth', *International Security* 38:2 (2013), 41–73.
Grissom, Adam, 'The Future of Military Innovation Studies', *Journal of Strategic Studies* 29:5 (2006), 905–934.
Gross, Micael, and Meisels, Tamar, eds., *Soft War, the Ethics of Unarmed Conflict* (Cambridge: Cambridge University Press, 2017).
Haass, Richard, 'How a World Order Ends: And What Comes in Its Wake', *Foreign Affairs* 98:1 (2019), 22–30.
Hedges, Chris, *War Is a Force that Gives Us Meaning* (New York: Public Affairs, 2002).
Helmus, Todd C., Bodine-Baron, Elizabeth, Radin, Andrew, Magnuson, Madeline, Mendelsohn, Joshua, Marcellino, William, Bega, Andriy, and Winkelman, Zev, *Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND, 2018).
Hill, Andrew, and Gerras, Stephen, 'Systems of Denial, Strategic Resistance to Military Innovation', *Naval War College Review* 69:1 (2016), 109–132.
Hoffman, Frank, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: The Potomac Institute of Policy Studies Arlington, 2007).
Hoffman, Frank, 'Neo-Classical Counterinsurgency?' *Parameters* 37:2 (2007), 71–87.
Hoffman, Frank, 'The Future Is Plural, Multiple Futures for Tomorrow's Joint Force', *Joint Force Quarterly* 88:1 (2018), 4–13.
Howard, Michael, *The Invention of Peace* (Hartford, CT: Yale University Press, 2000).

Hyde-Price, Adrian, 'European Security, Strategic Culture, and the Use of Force', *European Security* 13:4 (2004), 323–343.
Jackson, Richard, and Dexter, Helen, 'The Social Construction of Organized Political Violence: An Analytical Framework', *Civil Wars*, 16:1 (2012), 1–23.
Jakobsen, Peter Viggo, 'The Yugoslav Wars', in *Western Use of Coercive Diplomacy After The Cold War*, Peter Viggo Jakobsen, ed., 70–109 (London: Palgrave, 1998).
Jakobsen, Peter Viggo, *Western Use of Coercive Diplomacy after the Cold War* (London: Macmillan, 1998).
Johnson, David, *Hard Fighting: Israel in Lebanon and Gaza* (Santa Monica, CA: RAND, 2006).
Johnson, Robert A., 'Predicting Future War', *Parameters*, 44:1 (2014), 65–76.
Jones, Seth, *In the Graveyard of Empires: America's War in Afghanistan* (New York: W. W. Norton & Company, 2010).
Jones, Seth, 'The Future of Warfare is Irregular', *The National Interest*, 26 August 2018, at https://nationalinterest.org/feature/future-warfare-irregular-29672.
Jones, Seth, *Waging Insurgent Warfare, Lessons from the Vietcong to the Islamic State* (Oxford: Oxford University Press, 2016).
Juergensmeyer, Mark, *Terror in the Mind of God* (Berkeley: University of California Press, 2003).
Kagan, Robert, *Of Paradise and Power: America and Europe in the New World Order* (New York: Knopf, 2003).
Kaldor, Mary, *New and Old Wars* (Cambridge: Polity, 1999).
Kaplan, Robert, *The Coming Anarchy: Shattering the Dreams of the Post Cold War* (New York: Vintage Books, 2001).
Kaufman, Stuart, 'Symbolic Politics or Rational Choice? Testing Theories of Extreme Ethnic Violence', *International Security* 30:4 (2006), 45–86.
Kello, Lucas, *The Virtual Weapon and International Order* (Hartford, CT: Yale University Press, 2017).
Kilcullen, David, *Out of the Mountains, the Coming Age of the Urban Guerrilla* (London: Hurst, 2013).
Kilcullen, David, *The Accidental Guerrilla* (Oxford: Oxford University Press, 2009).
Kitzen, M.W.M., and Thönissen, F.H., 'Strategische vaagheid, Hoe het gebrek aan strategische visie het lerend vermogen van de Koninklijke Landmacht beperkt', *Militaire Spectator* 187:4 (2018), 206–223.
Krieg, Andreas, and Rickli, Jean-Marc, 'Surrogate Warfare: The Art of War in the 21st Century?' *Defence Studies* 18:2 (2018), 113–130.
Kroenig, Matthew, 'Facing Reality: Getting NATO Ready for a New Cold War', *Survival,* 57:1 (2015), 49–70.
Lanoszka, Alexander, 'Russian Hybrid Warfare and Extended Deterrence in Eastern Europe', *International Affairs* 92:1 (2016), 175–195.
Larson, Eric V., et al., *Foundations of Effective Influence Operations* (Santa Monica, CA: RAND, 2009).
Latiffe, Robert, *Future War, Preparing for the New Global Battlefield* (New York: Vintage Books, 2017).
Lemay-Hébert, Nicolas, 'Statebuilding without Nation-building? Legitimacy, State Failure and the Limits of the Institutionalist Approach', *Journal of Intervention and Statebuilding* 3:1 (2009), 21–45.
Libicki, Martin, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

Mac Ginty, Roger, and Richmond, Oliver P., 'The Local Turn in Peace Building: A Critical Agenda for Peace', *Third World Quarterly* 34:5 (2013), 763–783.
Mandelbaum, Michael, *The Rise and Fall of Peace on Earth* (New York: Oxford University Press, 2019).
McFate, Sean, *The New Rules of War: Victory in the Age of Durable Disorder* (New York: William Morrow, 2019).
Mehta, Rupal, 'Extended Deterrence and Assurance in an Emerging Technology Environment', *Journal of Strategic Studies* (2019). doi: 10.1080/01402390.2019.1621173
Mello, Patrick, 'National Restrictions in Multinational Military Operations: A Conceptual Framework', *Contemporary Security Policy* 40:1 (2019), 38–55.
Merom, Gil, *How Democracies Lose Small Wars* (New York: Cambridge University Press, 2003).
Monaghan, Sean, ed., *Countering Hybrid Warfare* (Shrivenham: DCDC, 2018).
Morris, Lyle J., Mazarr, Michael J., Hornung, Jeffrey W., Pezard, Stephanie, Binnendijk, Anika, and Kepe, Marta, *Gaining Competitive Advantage in the Gray Zone, Response Options for Coercive Aggression below the Threshold of Major War* (Santa Monica, CA: RAND, 2019).
Moskos, Charles, Williams, John Allen, and Segal, David, eds., *The Postmodern Military, Armed Forces After the Cold War* (Oxford: Oxford University Press, 2000).
Mudde, Cas, 'Europe's Populist Surge, A Long Time in the Making', *Foreign Affairs* 95:6 (2016), 25–30.
Mueller, J., *Retreat from Doomsday: The Obsolescence of Major War* (New York: Basic Books, 1989).
Mumford, Andrew, *Proxy Warfare* (Cambridge: Polity Press, 2013).
National Intelligence Council, *Global Trends Report, Paradox of Progress* (Washington, DC: National Intelligence Council, 2017).
Osinga, Frans, 'Bounding the Debate on Drone Warfare', in *Moral Responsibility & Military Effectivenes*, Herman Amersfoort, et al., eds., 243–278 (The Hague: Asser, 2013).
Osinga, Frans, 'De Strategische Pauze Voorbij: Veiligheid, Defensie en de Westerse krijgsmacht na 9/11', *Militaire Spectator* 180:9 (2011), 398–415.
Osinga, Frans, 'The Rise of Transformation', in *A Transformation Gap? American Innovations and European Military Change*, Terry Terriff, Frans Osinga, Theo Farrell, eds., 14–34 (Stanford, CA: Stanford University Press, 2010).
Osinga, Frans, Farrell, Theo, and Russell, James, eds., *Military Adaptation and the War in Afghanistan* (Stanford, CA: Stanford University Press, 2013).
Paris, Roland, 'The "Responsibility to Protect" and the Structural Problems of Preventive Humanitarian Intervention', *International Peacekeeping* 21:5 (2014), 569–603.
Paris, Roland, and Sisk, Timothy, *The Dilemmas of Statebuilding* (London: Routledge, 2009).
Paul, Christopher, *Counterinsurgency Scorecard, Afghanistan* (Santa Monica, CA: RAND, 2011).
Paul, Christopher, Clarke, Colin P., Beth, Grill, and Dunigan, Molly, *Paths to Victory: Lessons from Modern Insurgencies* (Santa Monica, CA: RAND, 2013).
Paul, T.V., *Asymmetric Conflicts: War Initiation by Weaker Powers* (Cambridge: Cambridge University Press, 1994).

Payne, Kenneth, *Strategy, Evolution and War, From Apes to Artificial Intelligence* (Washington, DC: Georgetown University Press, 2018).

Polyakova, Alina, and Boyer, Spencer P., *The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition* (Washington, DC: Brookings Institute, 2017).

Polyakova, Alina, and Haddad, Benjamin, 'Europe Alone, What Comes after the Transatlantic Alliance', *Foreign Affairs* 98:4 (2019), 109–120.

Porch, Douglas, *Counterinsurgency: Exposing the Myths of the New Way of War* (Cambridge: Cambridge University Press, 2013).

Porter, Patrick, 'Taking Uncertainty Seriously: Classical Realism and National Security', *European Journal of International Security* 1:2, 239–260.

Rid, Thomas, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

Rid, Thomas, and Hecker, Marc, *War 2.0: Irregular Warfare in the Information Age* (Westport, CT: Praeger, 2009).

Ringsmose, Jens, and Børgesen, Berit Kaja, 'Shaping Public Attitudes towards the Deployment of Military Power: NATO, Afghanistan and the Use of Strategic Narratives', *European Security* 20:4 (2010), 505–528.

Robinson, Linda, Helmus, Todd C., Cohen, Raphael C., Nader, Alizera, Radin, Andrew, Magnuson, Madeline, and Migacheva, Katya, *Modern Political Warfare, Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018).

Rochelle, Carl, 'NATO Grapples with "War by Committee"', *CNN*, 19 April 1999.

Rothkopf, David, 'The Cool War', *Foreign Policy*, 20 February 2013.

Sageman, Mark, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

Shimko, Keith, *The Iraq Wars and America's Military Revolution* (Cambridge: Cambridge University Press, 2010).

Shultz, Richard, and Dew, Andrea, *Insurgents, Terrorists and Militias, the Warriors in Contemporary Conflict* (New York: Columbia University Press, 2006).

Singer, Peter, *LikeWar, The Weaponization of Social Media* (Boston, MA: Eamon Dolan, 2018).

Smith, Rupert, and Bet-El, Ilana, *The Utility of Force, The Art of War in the Modern World* (New York: Knopf, 2005).

Snyder, Jack, 'The Broken Bargain, How Nationalism Came Back', *Foreign Affairs*, 98:2 (2019), 54–60.

Strachan, Hew, 'The Lost Meaning of Strategy', *Survival* 47:3 (2005), 33–54.

Strachan, Hew, *The Direction of War* (Cambridge: Cambridge University Press, 2013).

Taleb, Nassim Nicholas, *Antifragile Things that Gain from Disorder* (New York: Random House, 2014).

Tardy, Thierry, 'United Nations Protection Force (UNPROFOR—Bosnia and Herzegovina)', in*he Oxford Handbook of United Nations Peacekeeping Operations*, Joachim Koops, et al., eds., 371–394 (Oxford: Oxford University Press, 2015).

Toft, Monica Duffy, 'Ending Civil Wars, a Case for Rebel Victory?' *International Security* 34:4 (2010), 7–38.

Treverton, Gregory F., Thvedt, Andrew, Chen, Alicia R., Lee, Kathy, and McCue, Madeline, *Addressing Hybrid Threats* (Stockholm: Swedish Defence University, 2018).

US Army: Field Manual 3–24 Counterinsurgency (Washington, DC: Headquarters of the Department of the Army, 2006).

US General Accounting Office, *Kosovo Air Operations: Need to Maintain Alliance Cohesion Resulted in Doctrinal Departures* (Washington, DC: US General Accounting Office, 2001).

US Joint Forces Command, *Commander's Handbook for Strategic Communication and Communication Strategy* (Suffolk, VA: US Joint Forces Command, 2010).

Votel, Joseph L., and Keravuori, Eero R., 'The by-with-through Operational Approach', *Joint Force Quarterly* 89:2 (2018), 40–47.

Wasson, Jesse T., and Bluesteen, Christopher E., 'Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems', *Defence Studies* 18:4 (2018), 433–453.

Weitsman, Patricia, *Waging War, Alliances, Coalitions and Institutions of Interstate Violence* (Stanford, CA: Stanford University Press, 2014).

Wildavsky, Aaron, *The Real World Order: Zones of Peace/Zones of Turmoil* (Chatham: Chatham House, 1993).

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Part II

New strategies in the conduct of contemporary warfare

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

3 Hybrid warfare and counter-coercion

Rob Johnson

Introduction

The West had led in what seemed a new way of war by using their air power and Special Forces to 'enable' local militia in the form of Afghan anti-Taliban irregulars (2001), the Kurdish 'peshmerga' (2003), and then Libyan rebels (2011) to achieve parallel objectives. The same model was used to assist Iraqi regular armed forces against the so-called Islamic State (2015), although conventional ground forces were required too. In the latter case, Western states had also carefully calibrated information warfare and cyber activities with their use of airpower and ground contingents. This combination simultaneously degraded their enemies' capabilities, broke their physical grip on a region in high tempo joint operations, and discredited their adversaries' prestige and authority.

The combination of conventional and unconventional techniques to change the geopolitical landscape occurred at a time when large-scale conventional war seemed unthinkable. The success of the 'hybrid' approach in the early 2000s fulfilled the theoretical speculation of the previous decades, including the idea of 'Unrestricted Warfare' or '4th Generation Warfare'. Russia was particularly alarmed by the phenomenon, believing that events like the Arab Spring (2011) or pro-European unrest in Kiev (2014) were orchestrated by the West as induced 'colour revolutions.'[1] General Valery Gerasimov warned his countrymen of the threat this posed in a celebrated article in 2013.[2] That publication seemed to indicate that Russia, eager to restore its military power and international standing, was about to conduct its own hybrid warfare against the West.

Russian actions in the Caucasus in 2008, against Estonia in 2013, and then the illegal annexation of the Crimea by force in 2014, using unidentifiable troops and frequent diplomatic denials, prompted considerable debate in NATO, whose military was but a shadow of its Cold War capability.[3] China too seemed more confident in orchestrating a campaign of coercion using economic pressure, naval intimidation using warships disguised as 'coastguard', and threats of retaliation in the South China Sea.

Scholars joined the discussions. David Kilcullen explained that the United States was still confident in its conventional military power and saw

no need to adapt, which left it ineffective in face of hybrid warfare.[4] In 2015, Nadia Schadlow lamented the lack of progress in operational considerations to counter hybrid warfare.[5] Concurrently, there was growing concern about the 'weaponizing' of other means, particularly information.[6] Western states were soon investigating how they might use military force to complement the exercise of power across several domains in situations short of war, to counter hybrid warfare.

This chapter clarifies the term 'hybrid warfare' and then considers the changes in the conduct of war that hybrid operations represent. The last section of this brief analysis examines the countering of coercive operations that came under the definition of hybrid in the 2010s, before concluding with some reflections on the changes that have occurred, juxtaposing those with the more familiar characteristics of state coercion and the dilemmas that surround the use of force.

From combined operations to decomposition of cohesion and morale

Observing the tendency of irregular actors to make use of modern technologies, while being mobilised by a reckless, ideological fervour, Frank Hoffman coined the term multi-modal, or hybrid warfare to describe fighting styles without orthodox structures or obedience to the laws of armed conflict.[7] After Hoffman, the term developed and was seen as a blend of conventional and unconventional tactics which could be used to further national objectives without crossing a recognised threshold of armed conflict such as NATO's Article 5.[8] In all cases, hybrid warfare focussed on 'ways' and 'means'.

Hoffman subsequently developed a more holistic view of hybrid warfare. He argued that 'new wars, open source warfare, [post-]modern wars, polymorphic conflict, combinational wars, and Fourth Generation Warfare' were the antecedent concepts that both informed and stymied the thinking that led to the emergence of the term 'hybrid warfare'.[9] He stated: 'Hybrid warfare is different because it addresses the difference in "how" the adversary plans to fight'.[10] The very hybridity of the types of ways, means, and actors seems to incorporate both state and non-state use of the approach, and therefore more easily conceptualises a variety of tools as combined instruments of state power. These can be used to shape an objective during a time of peace or be used more coercively in times of conflict. Hoffman concludes: '[There is an] increased merging … of conflict and war forms. The potential for types of conflict that blur the distinction between war and peace, and combatants and non-combatants, appear to be on the rise'.[11] As an operational concept, Hoffman believes these hybrid elements require a level of centralised control. They have to be coordinated and directed to achieve operational synergy, and thus work towards military and political objectives. This implies the existence of a coordinated strategy, which, regardless of the opaque or opportunistic ways and means, suggests very clear ends.

Hoffman took the original idea of blended actors and coordinated effects to include both physical and psychological dimensions of conflict, emphasising the Clausewitzian objective of war: to reduce the ability and the will of an enemy to resist. Therefore, according to Hoffman, in the military sphere, hybrid adversaries use, simultaneously, a mix of conventional forces, conventional and irregular tactics, terrorism, and criminal behaviour to obtain their political objectives. These are directed and coordinated to achieve synergistic effects in the physical and psychological dimensions of conflict.[12] He supports this with observations of the coercive effects that can be achieved through non-state armed groups, such as criminal organisations and terrorists, during a time of 'peace', that is, under peacetime norms.[13] The value of Hoffman's later insights is that he brings us back from 'ways' to the 'ends' of war – in this case, to break down the cohesion and resilience of the targeted polity.

For those who find some utility in the concept of hybrid warfare, there are two general schools of thought. The first group believes that while hybrid warfare is a useful concept, it is not new.[14] They contend that hybrid warfare is simply the *combination of regular and irregular forces* on the battlefield; irregulars being defined as militia, guerrillas, insurgents, and terrorists. The U.S. Army *TRADOC G-2* expands this list slightly to include:

> two or more of the following: military forces, nation-state paramilitary forces (such as internal security forces, police, or border guards), insurgent organizations (movements that primarily rely on subversion and violence to change the status quo), guerrilla units (irregular indigenous forces operating in occupied territory), and criminal organizations (such as gangs, drug cartels, or hackers)

with a heavy emphasis on the use of cyber operations.[15]

The second school of thought has numerous definitions for what can constitute hybrid warfare. Most of these definitions include conventional and irregular *forces* but give special categorisation to the operational reach of terrorism, and then include a wide variety of innovative approaches to applying technology and resourcefulness to negate an opponent's military superiority. This dynamic is considered to be a form of asymmetric warfare.[16] Others, within this school of thought, define 'hybrid' as the various *battlespaces* in the information warfare domain, where actors attempt to win influence over the 'populations in the conflict zone, on the home front, and in the international community'.[17] The unifying idea of this second school of thought is the novelty of hybrid warfare and therefore the requirement to develop entirely new responses to it.

Continuities and changes

Hybrid warfare, coercion short of war and periods of confrontation were all common historically, and combined effects were a feature of apparently

'conventional' wars.[18] But it was anxiety about the eroding of Western dominance in the 2010s that allowed notions of hybrid warfare to flourish. The aggressive posture of Russia in the period after 2008 and the concurrent growth of Chinese military power, particularly China's insistence on fortifying an island chain in the South China Sea to reinforce its claims to sovereignty, were at the centre of the debate. The virulence and frequency of mass-casualty terrorist attacks against civilians around the world, often fuelled by the violent transnational ideology of militant Islam, merely added to the sense of unease in Western capitals. Commentators regretted the lack of effective counter-measures, claiming that Western states were tied down by legal and ethical constraints, or that the confusing nature of hybrid threats made them almost impossible to check.

In 2010, the U.S. Secretary of Defense, Robert Gates, used the term hybrid warfare in the Quadrennial Defense Review to describe the sophisticated means that both state and non-state actors would employ to mitigate a conventional disadvantage against the United States.[19] Under the heading 'Shifting Operational Landscape' there were general descriptions of a hybrid threat that included: 'protracted forms of warfare, use of proxy forces for coercion and intimidation, terrorism and criminality to manipulate the information environment, target energy resources, attack economic vulnerabilities and exploit diplomatic leverage'.[20] This description covered a range of 'means' that might be employed by an aggressor as well as potential 'ways' and targets, but they did not define the actor or connect the potential targets to a coherent strategic intent. Without this framework, hybrid warfare is indistinguishable from other manifestations of irregular, asymmetric, or unconventional operations, and appeared to have no solution. But such a pessimistic view was misplaced. In the decade that followed, there were examples of where hybrid operations were countered, both in military operational terms and strategically.

The conduct of hybrid operations

Various hybrid warfare activities are united by the intent to pursue strategic ends with a degree of force, but not such an overt use of military force that it would cross the threshold of conventional justifications for war and thereby necessitate a military response. Russia's use of unidentifiable troops, sabotage, assassination, *coup de main*, the use of proxies (such as Wagner Group and other paramilitaries), and brinkmanship (including overflights of national airspace, or thinly disguised military forces) during its operations in Ukraine's Crimea and Donbass in 2014 did not, individually, justify the military response of the entirety of the NATO Alliance.

The military aspect of hybrid coercion invariably involves combined or blended political actions with unconventional 'ways', including disinformation campaigns, denials or dismissals of support for irregular proxies or psychological pressure. The purpose is to break down the cohesion, willpower,

or ability to make decisions of a targeted actor. If this is unsuccessful or requires a final toppling action, then limited but rapid military operations may follow to confront an enemy with a *fait accompli*. On the other hand, one might see attempts to draw an opponent into a fatal decision, so-called 'reflexive control', or a distracting sustained conventional operation in one theatre that opens up opportunities in another location.

The point is that military activities will not appear in isolation. This form of warfare is conducted with a mixture of 'means' of which the military may support or periodically lead depending on the effect or leverage desired. Information activities are particularly prominent, seeking to divide, demoralise, or discredit existing authorities. The hybrid-coercive attacker exercises deception, vociferous denials, and spurious accusations, seeking to achieve changes to 'facts on the ground' regardless of the debates in international institutions. The combination of approaches, on so many different axes, makes a coherent response seem difficult.

David Kilcullen refers to the doubt and hesitancy to use force in countering hybrid operations as a result of 'liminal warfare'.[21] He reiterates the centrality of psychological preparation and the manipulation of timing. His studies indicate that Russia will then seek to act and conclude an operation before the West can mount a response, and he cites Moscow's military doctrine to reinforce the point.

Similarly, analysts observe that China favours a notion of a continuous state of war, but one that is not always 'kinetic' in nature. The concept of people's war emphasises the combined use of political and military instruments and use of the 'Three Warfares': psychological, informational, and legal manipulation.[22] These are used to project psychological pressure, publicise its alleged 'legal' arguments, and assert China's claims to resources and territory, with the military providing intimidation. It is interesting to note that from the outset communist China has made use of deception and the concealment of its forces' identity without insignia, as in the Korean War. On the other hand, China's 'social credit system' and other forms of domestic control indicate what Beijing fears most – large-scale domestic unrest, which has traditionally been China's greatest weakness.

The West's military culture, which was based on 'conventional' warfare, risked failure under these conditions. Peacetime rules in situations of evident confrontation and coercion could still potentially jeopardise success and increase hazard, while purporting to reduce it. It is striking how the covid-19 in 2019–2020 underscored the impact of wartime conditions on Western states and exposed its critical vulnerabilities in countering unorthodox threats like bio-warfare. The solution lay in an integrated response, and steps have been taken, across the Western alliance, to address the threats. NATO has established, for example, Centres of Excellence devoted to the study of hybrid warfare and cyber activities. The EU has established principles of security, and NATO member states concluded a Cyber Pledge in 2018 to counter malign activity. A new consciousness developed, heightened by

the assertive diplomacy of China during the covid-19 pandemic, of the strategic threat to Western economies and the challenge of their dependence on supply chains or businesses that were at the behest of Beijing's authoritarian government.

Nevertheless, countering hybrid warfare is not limited to NATO and its partners against Russian or Chinese coercion. In 2006 Hezbollah used hybrid tactics against the Israeli Defence Forces (IDF), and, although it suffered a succession of defeats, it conveyed the impression of success, a point reinforced by Israel's self-critical appraisal of its own tactical performance. What caught the media's attention was Hezbollah's synchronised use of information operations and kinetic attacks.[23] It was well equipped with a large number of missiles and rockets, some unmanned aerial vehicles (UAVs), and anti-tank weapon systems. It had studied the Iraqi insurgent operations in Fallujah two years before and arranged urban ambushes along similar lines, co-locating its fighters with civilians as shields. Even though it lost its engagements with the IDF, Hezbollah's propaganda campaign and media footage made it seem it had inflicted catastrophic losses on Israel and effectively 'won' the campaign.[24] The messaging played well with the Arab world and persuaded the global media, institutions that are often dependent on readily available visual news feeds.

The IDF rectified the deficiencies in its operations when it fought against Hamas in 2009. The Israelis provided a continuous feed of media-worthy information on ground operations, held journalists in pools away from the battlefront, and synchronised social media releases prior to and after airstrikes. When confronted by mortar teams and fighters who were collocated with civilians, the IDF provided the photographic evidence of Hamas deployments which contravened the Law of Armed Conflict. Military operations were comprehensive, precise, and effective.

In 2015, as a new wave of violence swept out of Syria into Iraq, President Obama claimed that Islamic State (IS) was a new phenomenon, a 'sort of hybrid of not just the terrorist network, but one with territorial ambitions, and some of the strategy and tactics of an army', as he put it. Its fighting techniques, influenced by insurgencies in Chechnya and Iraq, combined conventional methods and illegal ones, including chemical weapon attacks and human shields, or devastating, large-scale vehicle-borne improvised explosive devices (VBIEDs) to create terror amongst their enemies. Their propaganda messaging was extensive, if somewhat traditional, inviting foreign fighters to join the movement, while seeking to discredit their adversaries by manipulating the iconography of Islam. IS financing included expropriations, theft, looting, smuggling, kidnapping for ransom, and illegal taxation. Its opposition was eliminated in large numbers, and areas that could mount an effective resistance were 'ethnically-cleansed'. The unconventional and illegal measures IS used, alongside its desire to acquire and hold territory and impose a militaristic dictatorship, were characterised as hybrid warfare.

The counter-measures included considerable military force reinforcing the point that, while coercive measures can be countered short of war, in actual armed conflict, there can be no escaping the necessity for force.[25] IS was defeated by an extensive air interdiction campaign and in ground operations, including dense urban settings, by a combination of air strikes, artillery fire, and armoured assaults with close quarter fighting by regular forces and irregulars. Neighbouring states, the Western Coalition, local groups, and the Syrian and Iraqi governments brought to bear considerable resources against IS. There was disruption of IS financing systems, destruction of smuggling convoys, the shutting down of media outlets, and counter-IS information warfare. In this, local civilians were crucial. The desire to avoid large-scale intervention or anti-Islamic policies coloured Western views about the level of force used, with precision air strikes, and the need to avoid or minimise civilian casualties. It therefore kept the ground commitment to a minimum.

Countering hybrid warfare and coercion after 2014

The Western response to the coercive actors has been strategic, with a clear role for military force. While military escalation might be considered the default response, it has been possible to assert strategic penalties through sanctions, diplomatic condemnation, isolation, and strategic positioning alongside allies and partners, from Finland to Saudi Arabia.[26] To ensure rapid reaction and fast deployment, there have been announcements of improvements to interoperability, new equipment programmes, a new emphasis on armour and missile capabilities on land, and new spending objectives to ensure modernisation. Western allies have rehearsed the ability to bring in more force rapidly to threatened zones such as the Baltic and Eastern Europe. The deployment of sufficient military force to signal the West's intent, without undue costs, creates a deterrent effect. Enhanced capabilities in surveillance, counter-cyber, in airpower, and in readiness of forces to mobilise and roll in within 30 days to any minor localised incursion further combine to deter. Military forces continue to initiate arranging and shaping operations, rehearsing information operations, to disrupt, delay, mislead, and otherwise impose friction. They can, if necessary, interfere with hostile enemy communications. They can deploy fire power showing its readiness for use, including exercises involving nuclear weapons such as the US and UK's continuous at sea nuclear deterrent (CASND). They examine the most efficient neutralisation of an enemy's command, control, and communications, the protection of operational security, and confidence-building of one's own forces and public.

Western operational commanders are anxious to know what opportunities lie in 'hybrid warfare' for them in an offensive as well as a defensive setting, and how to overcome the friction for the civil direction of the military instrument under conditions of hybrid coercion or confrontation. Their

expeditionary posture, namely their ability to project power across the globe, and effective mobile, heavily armed, and 'decisive battle'-oriented forces may have seemed to have made it harder to adapt to the new conditions.[27] But Western forces are still a powerful, and now more rapidly deployable, adversary to reckon with. The evolution of sophisticated robotic and automated tools may increase the gap between advanced Western forces and their challengers. Nevertheless, this will, in turn, push state and non-state armed actors to develop more clandestine and unconventional methods such as the ones currently described as hybrid or 'unrestricted'. In other words, this phenomenon is likely to exist for some time.

The verdict on countering hybrid warfare and peacetime coercion is therefore mixed. David Kilcullen believed that hybrid warfare was favoured by states challenging the West because it offered a way to degrade overwhelming Western military power.[28] He wrote:

> new actors with new technology threaten[ing] new or transfigured ways of war, but the old threats also remain and have to be dealt with in the same time and space, stressing the resources and overloading the systems of western militaries.[29]

Concentrating on the tactical level, Kilcullen showed that both state and irregular forces employ any variety of weapons and tactics to 'minimize detection and retaliation'.[30]

Hybrid warfare to some extent reflects new opportunities in the conduct of war at both the strategic and operational level due to the combined effects of globalisation, connectivity, mass communications that gives access to the world's population, and the technological innovations of the internet, mobile telephony, and cable and satellite television. It reflects the deliberate choice of a state or non-state actor to utilise the options of asymmetry, limited war, or unconventional means and ways.

In a coercive situation short of war, traditional military forces still have a role that can be significant, but they may also play a secondary role, providing sufficient force at a specific time and place to create the required media or psychological effect. The plausible threat of overwhelming force may be an important component, but conventional military formations are, at times, likely to be the less important element in these situations. Their role may be an enabling one, a deterrent, a facilitator of local actors, a deception, or a rapid reaction force.

Clausewitz' dictum that war is 'a continuation of politics, with an admixture of other means' is often thought to mean that a distinct moment is reached where political and diplomatic activity stops and military operations begin.[31] In fact, all war, not just hybrid warfare, is never so clearly demarcated. In countering coercion and hybrid warfare, the military instrument has an important role to play, adding credibility to deterrence, denying options to an adversary, and, ultimately, narrowing their policy

choices. In developing a robust strategic response to coercion, the synchronisation of military and other means could provide a significant strategic advantage.

Reflections on the military role in counter-coercion, counter-hybrid operations

Paul Brister described hybrid warfare as a form of limited war for strategic ends:

> The aim of military strategy is to create a dilemma for the enemy, and make him choose which objective he will defend, a challenge in the modern era due to the isolation of numerous potential objectives from interdiction by military force.[32]

The objective is more easily understood as a set of actions that shape a situation, to *deny* as well as compel choice, but which also create opportunities where, perhaps, military means are not required at all.[33] Counter-measures need not be limited by the term 'warfare'. It can enable one to impose friction and costs on an adversary using coercion to negate their strategic benefit. The objective is to widen one's own options, whilst limiting an opponent's. It is the fulfilment of policy, while denying an enemy the achievement of his.

This form of coercion before full scale hostilities would have been recognisable to George Kennan as 'political warfare', which described the employment of all the means at a nation's command, short of war, to achieve its national objectives.[34] The conduct of hybrid war, when the fighting has broken out, will invariably make use of political and informational ways and means, or unconventional methods to augment military power. In this sense, much remains unchanged from the past.[35] The art of hybrid war continues to demand centralised co-ordination, careful synchronised calibration, and clear political objectives.

Notes

1 Rob Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies*, 29:1 (2018), 141–163, Alexander George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (Washington, DC: United States Institute of Peace Press, 1991).
2 Charles Bartles, 'Getting Gerasimov Right', *Military Review*, 96:1 (2016), 30–38.
3 Bettina Renz, 'Russia and "Hybrid Warfare"', *Contemporary Politics* 22:3 (2016), 283–300. https://doi.org/10.1080/13569775.2016.1201316 (Accessed January 2020).
4 David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford; New York: Oxford University Press, 2009), 2–3.
5 Nadia Schadlow, 'The Problem with Hybrid Warfare', *War on the Rocks* (April 2015) http://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/ (Accessed April 2015).

6 Nathan P. Freier, *Known Unknowns: Unconventional "Strategic Shocks" in Defense Strategy Development* (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2008), 34.
7 Frank Hoffman, 'Hybrid Warfare and Challenges', *Joint Forces Quarterly*, 52:1 (2009), 34–39. See also: Frank G. Hoffman, 'Hybrid versus Compound War: The Janus Choice Defining Today's Multifaceted Conflict', *Armed Forces Journal* (October 2009), 15.
8 Frank Hoffman, 'Hybrid Threats: Reconceptualising the Evolving Character of Modern Conflict', *Institute for National Strategic Studies Forum*, 240 (April 2009), Frank Hoffman, 'Hybrid Warfare and Challenges', *Joint Forces Quarterly* 52 (first quarter, 2009), 34–39; Frank Hoffman 'Hybrid vs Compound Wars', *Armed Forces Journal* (October 2009); John J. McCuen, 'Hybrid Wars', *Military Review* (March–April 2008).
9 Hoffman, 'The Hybrid Character of Modern Conflict', 37–38.
10 Ibid., 38. Hoffman highlights 'how' the adversary plans to fight, or the strategic 'ways' that the 'means' will be employed, and his definitions are a blend of these in terms of conventional, irregular (ways and means), terrorism (ways and means), and criminal activity (ways).
11 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 7.
12 Hoffman, *The Hybrid Character of Modern Conflict*, 40.
13 Hoffman, F.G. ''Hybrid Threats': Neither Omnipotent Nor Unbeatable', *Orbis* 54:3 (2010), 441–455. https://doi.org/10.1016/j.orbis.2010.04.009 (Accessed February 2020).
14 Peter R. Mansoor, 'Hybrid Warfare in History', in Williamson Murray and Peter R. Mansoor eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (New York: Cambridge University Press, 2012), 1–17.
15 TRADOC (US Army Training and Doctrine Command) G-2, 'Operational Environments to 2028: The Strategic Environment for Unified Land Operations' (August 2012), 5.
16 Timothy McCulloh and Richard Johnson, 'Hybrid Warfare', *JSOU Report* 13–14 (August 2013); Nathan P. Freier, *Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2007).
17 Jack McCuen, 'Strategy of Hybrid War', in Paul Brister, William H. Natter and Robert R. Tomes, eds., *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict* (New York: Council for Emerging National Security Affairs, 2011), 70–82.
18 Williamson Murray and Peter R. Mansoor, eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge University Press, 2012).
19 Robert M. Gates, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, 2010).
20 Ibid.
21 David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (London: Hurst, 2020), 158–159.
22 Andrew Scobell, 'The Chinese Way of War', in John Andreas Olsen and Martin van Creveld, eds., *The Evolution of Operational Art: From Napoleon to the Present* (Oxford: Oxford University Press, 2010), Stefan Halper, ed., *China: The Three Warfares*, https://cryptome.org/2014/06/prc-three-wars.pdf (Accessed March 2020), Rush Doshi, 'China Steps Up Its Information War in Taiwan', 9 January 2020, https://www.foreignaffairs.com/articles/china/2020-01-09/china-steps-its-information-war-taiwan (Accessed February 2020).

23 Paul Scharre, 'Spectrum of What?' *Military Review* (November 2012), 76; Alex Deep, 'Hybrid War: Old Concept, New Techniques', *Small Wars Journal* (March 2015), David Simon-Tov and Yoram Schweitzer, 'Israel against Hizbollah: Between Overt and Covert Warfare', *INSS Insight*, 668 (March 2015).
24 Kilcullen, *The Dragons and the Snakes*, 96–112.
25 Scott Jasper and Scott Moreland, 'The Islamic State Is a Hybrid Threat: Why Does That Matter?', *Small Wars Journal* (December 2014).
26 This maintained a limited war approach. Peter Paret and Daniel Moran, eds. and trans., 'Carl von Clausewitz: Two Letters on Strategy' (Combat Studies Institute, 1984), 1–3.
27 Lawrence Sondhaus, *Strategic Culture and Ways of War* (London: Routledge, 2009).
28 Kilcullen, *The Accidental Guerrilla*, 5–6.
29 Ibid.
30 David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013), 105.
31 Carl von Clausewitz, *On War*, Michael Howard, Peter Paret, eds. and trans. (Princeton, NJ: Princeton University Press, 1976), 606–607.
32 Paul Brister, 'Revisiting the Gordian Knot: Strategic Considerations for Hybrid Warfare', in Paul Brister, William H. Natter, and Robert R. Tomes, eds., *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict* (New York: Council for Emerging National Security Affairs, 2011), 51.
33 Ronald R. Luman, 'Introduction', in Ronald R. Luman, ed., *Unrestricted Warfare Symposium: Proceedings on Strategy, Analysis, and Technology* (Laurel, MD: Johns Hopkins University, Applied Physics Laboratory, 2006), 2.
34 George F. Kennan, *The Inauguration of Organized Political Warfare* (Washington, DC: Central Intelligence Agency, 1948). The Soviet Union used a wide range of measures to achieve their ends, including 'agitprop' (agitation propaganda), 'wet operations' (assassination), 'active measures' and 'reflexive control' (goading, provoking and luring actions along predetermined, prepared lines following study of likely and known behaviour).
35 Colin S. Gray, *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2006), 4.

References

Alexander, George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (Washington, DC: United States Institute of Peace Press, 1991).

Bartles, Charles, 'Getting Gerasimov Right', *Military Review* 96:1 (January 2016), 30–38.

Brister, Paul, 'Revisiting the Gordian Knot: Strategic Considerations for Hybrid Warfare', in *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict*, Paul Brister, William H. Natter and Robert R. Tomes, eds. (New York: Council for Emerging National Security Affairs, 2011), 14–26.

Chaudhuri, Rudra and Farrell, Theo, 'Campaign Disconnect: Operational Progress and Strategic Obstacles in Afghanistan, 2009–2011', *International Affairs* 87:2 (2011), 271–296.

Clausewitz, Carl von, *On War*, Michael Howard, Peter Paret, eds. and trans. (Princeton, NJ: Princeton University Press, 1976).

Deep, Alex, 'Hybrid War: Old Concept, New Techniques', *Small Wars Journal* (March 2015).

Doshi, Rush, 'China Steps Up Its Information War in Taiwan', *Foreign Affairs* 9 January 2020, https://www.foreignaffairs.com/articles/china/2020-01-09/china-steps-its-information-war-taiwan (Accessed February 2020).

Freier, Nathan P., *Known Unknowns: Unconventional "Strategic Shocks" in Defense Strategy Development* (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2008).

Freier, Nathan P., *Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2007).

Gates, Robert M., *Quadrennial Defense Review Report* (Washington, DC: Dept. of Defense, 2010).

Gray, Colin S., *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2006).

Halper, Stefan, ed., *China: The Three Warfares*, https://cryptome.org/2014/06/prc-three-wars.pdf (Accessed March 2020).

Hoffman, Frank G., *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).

Hoffman, Frank G., "'Hybrid Threats': Neither Omnipotent Nor Unbeatable." *Orbis* 54:3 (2010), 441–455, https://doi.org/10.1016/j.orbis.2010.04.009 (Accessed February 2020).

Hoffman, Frank G., 'Hybrid Threats: Reconceptualising the Evolving Character of Modern Conflict', *Institute for National Strategic Studies Forum*, 240 (April 2009), 1–8.

Hoffman, Frank G., 'Hybrid versus Compound War: The Janus Choice Defining Today's Multifaceted Conflict', *Armed Forces Journal* (October 2009). http://armedforcesjournal.com/hybrid-vs-compound-war/

Hoffman, Frank G., 'Hybrid Warfare and Challenges', *Joint Forces Quarterly* 52:1 (2009): 34–39.

Jasper, Scott, and Moreland, Scott, 'The Islamic State Is a Hybrid Threat: Why Does That Matter?' *Small Wars Journal* (December 2014).

Johnson, Rob, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars & Insurgencies* 29:1 (2018), 141–163.

Kennan, George F., *The Inauguration of Organized Political Warfare* (Washington, DC: Central Intelligence Agency, 1948).

Kilcullen, David, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013).

Kilcullen, David, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford; New York: Oxford University Press, 2009).

Kilcullen, David, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (London: Hurst & Co., 2020).

Luman, Ronald R., 'Introduction', in *Unrestricted Warfare Symposium: Proceedings on Strategy, Analysis, and Technology*, Ronald R. Luman, ed. (Laurel, MD: Johns Hopkins University, Applied Physics Laboratory, 2006), 1–10.

Mansoor, Peter R., 'Hybrid Warfare in History', in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Williamson Murray and Peter R. Mansoor, eds., 1–17 (New York: Cambridge University Press, 2012).

McCuen, Jack, 'Strategy of Hybrid War', in *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict*, Paul Brister, William H. Natter and Robert R. Tomes, eds., 70–82 (New York: Council for Emerging National Security Affairs, 2011).

McCuen, John J., 'Hybrid Wars', *Military Review* (March–April 2008).

McCulloh, Timothy, and Johnson, Richard, 'Hybrid Warfare', *JSOU Report* 13–14 (August 2013).

Murray, Williamson, and Mansoor, Peter R., eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge: Cambridge University Press, 2012).

Paret, Peter, and Moran, Daniel, eds. and trans., 'Carl von Clausewitz: Two Letters on Strategy', (Combat Studies Institute, 1984).

Renz, Bettina, 'Russia and 'Hybrid Warfare'', *Contemporary Politics* 22:3 (2016): 283–300 https://doi.org/10.1080/13569775.2016.1201316 (Accessed January 2020).

Schadlow, Nadia, 'The Problem with Hybrid Warfare', *War on the Rocks* (April 2015), http://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/ (Accessed April 2015).

Scharre, Paul, 'Spectrum of What?' *Military Review* (November 2012), 73–79.

Scobell, Andrew, 'The Chinese Way of War', in *The Evolution of Operational Art: From Napoleon to the Present*, John Andreas Olsen, Martin van Creveld, eds. (Oxford: Oxford University Press, 2010), 195–221.

Simon-Tov, David, and Schweitzer, Yoram, 'Israel against Hizbollah: Between Overt and Covert Warfare', *INSS Insight*, 668 (March 2015). https://www.inss.org.il/publication/israel-against-hizbollah-between-overt-and-covert-warfare/

Sondhaus, Lawrence, *Strategic Culture and Ways of War* (London: Routledge, 2009).

US Army Training and Doctrine Command, G-2, 'Operational Environments to 2028: The Strategic Environment for Unified Land Operations' (August, 2012).

4 Strategies for communicating information and disinformation in war

Managing and exploiting uncertainty in social media

Filippo Tansini and Yakov Ben-Haim

Introduction

States engage in diverse types of strategic public communication during armed conflict or crisis, with various goals and facing a range of uncertainties. We compare two distinct methodologies for designing strategic communications. The first methodology focuses on optimising the outcome of the strategic communications, based on a model of the information environment. The second methodology, based on info-gap decision theory, satisfies outcome requirements and optimises the robustness to uncertainty (rather than optimising the outcome). We identify situations in which one strategy, or the other, is preferable.

Ivana Marková in 2008 wrote: 'There would be hardly any reason to communicate if there were no tensions, asymmetries or conflicts between interacting parties'.[1] From a psychosocial perspective, every conflict motivates communication. For instance, dominating groups may try to reduce internal conflict by identifying external enemies through propaganda. While the fundamental nature of warfare may be constant through history, the character of war has changed over time. Variations in conduct of war can be found in the type of actors involved (asymmetry between contenders as opposed to symmetric conflict of States), in their purpose (economic, ethnic identity, personal, political or religious motives), in conflict localisation and extension (urban low intensity vs. global conflict). Variations in characteristics of war create diverse information landscapes, with new communication needs and opportunities. The modern digital information environment creates what Luciano Floridi defined as our contemporary 'on-life'.[2]

Unlike clashes for survival, contemporary war is frequently 'war of choice'.[3] The 'choice' for conflict is almost inevitably questionable and becomes disputed regarding its opportunity, quality and legitimacy. Consequently, every actor involved (nation-state, irregular fighter or terror group) struggles to establish a widespread and prevailing narrative over its choice, before, during and after the conflict. Control of the narrative is a critical ambition of every actor involved in contemporary conflicts.

Digital and social media are often used for tactical and strategical information management during conflicts. Indeed, in 2017, 'Information' was introduced as a Joint Function in the Doctrine for the Armed Forces of the United States, where its pervasive nature is described through an axiom reminiscent of the basic rules of communication: 'all military activities produce information'.[4] The doctrine argues that, because almost all decision making and behaviour relies on communication, the influence of information will inevitably impact strategic outcomes.[5]

Information operations are currently described in JP 3-13 as entailing five activities: Computer Network Operations, Psychological Operations, Electronic Warfare, Operations Security and Military Deception. The relationship between information operations and information warfare is explained in a Congressional Research Service report: 'strategy can be defined as the process of planning to achieve objectives and goals in the national interest. Operations link strategic objectives with tactics, techniques, and procedures. For Information Warfare strategy, that link is Information Operations'.[6]

The aforementioned field of actions, together with strategic communication, diplomacy, public affairs and civil initiatives, can all be analysed together as different operational sides of a multi-faceted landscape, namely the information environment. This composite horizon is the realm where information warfare (and all its subsequent functional areas) takes place. It could be roughly defined as: who's saying what to whom, using which medium and gaining what effects.

Information operations in all their manifestations are realised in different real-world scenarios: influencing outcomes of foreign elections, ensuring domestic support for initiating hostilities, degrading internal cohesion among enemy troops, protecting one's own operational security or deceiving opponents to gain advantage in specific battles. These examples all require quite similar implementation as communication strategies and subsequent management activities. Nonetheless, their diverse complexity exposes each outcome to various degrees of uncertainty.

The complexity of desired outcomes of an information operation is the main independent variable. It actively determines the exposure of objectives to known and unknown degrees of risk. The scale of the outcome varies from tactical to strategic in nature, and uncertainties vary from shallow to deep. Whether and how an information operation should seek the putatively best possible outcome will be the focus of this chapter.

Field of battle, available knowledge and major uncertainties

In NATO Allied Joint Doctrine for Information Operations the bond between information and the contemporary digital revolution is defined as 'revolutionary'.[7] The need for legitimacy pervades every modern conflict, and the media play pivotal roles in shaping the informational landscape and influencing global perceptions. The digital information landscape and

social media in particular introduce great uncertainties in the mythopoesis of reasons to fight.

Social media dynamics have deep impact in defining the audience that is interested in a crisis and its perception of time, space and involvement. Collings and Rohozinski identified six characteristics of social media regarding their effects on the established communication field: they are pervasive, ubiquitous, instantaneous, interactive, social and specific, and 'sticky'.[8]

Pervasiveness: social media, micro-blogging platforms and discussion boards increase their diffusion among citizens every year in almost every country. Access to them is increasingly performed through mobile and portable devices, making it even more pervasive.

Ubiquity: Time and space become almost meaningless attributes: every action within the (virtual) 'theatre of operations' can have instantaneous diffusion and immediate feedback from users located in every country in the world.[9]

Instantaneousness and interactivity: Social media and new media interact as a near-real-time distributed cycle of content co-creation and diffusion.

Social and specific: Their nature is personal and direct. Along with the described usage routines, they enable the development of new information activities (citizen journalism, activism/hacktivism, blogger and influencer) and the appearance of distinctive information dynamics.[10]

Stickiness: The joint effects of these five traits create a complex system of information with the emergence of the sixth unexpected quality of stickiness: a specific communicative dynamics regarding citizens' trustfulness and news consumption:

> consumers become participants in the information-making process, following or participating in stories as they develop, which contributes to a positive sense of crowd sourcing and seemingly avoids the perceived bias of old media (where information is thought to be filtered).[11]

These six features add elements of severe unpredictability and make the digital battlefield unavoidable to anyone wishing to operate within the contemporary information environment.

These doctrines identify stages for implementing information operations to obtain desired outcomes. The common phases are situation awareness, planning and executing, and assessing results of the operation. We now discuss these phases, highlighting known elements, and considering whether or how (explicitly or implicitly) these doctrines deem the social media landscape to be fundamentally uncertain.

Situational awareness

The joint doctrine of the United Kingdom Defence Ministry reduces information operations to minimal terms: it relies on every activity whose primary purpose is influencing the will. This is done by communicating

specific themes through messages tailored to defined target audiences.[12] This definition implies that Target Audience Analysis (TAA) is the first step towards defining a communication strategy. Similarly, the US and NATO suggest comprehensive analysis of the information environment as composed of basic encyclopaedic information about the crisis area (political, security, economic, social and infrastructure systems) and detailed analysis of the informational landscape: 'psychological, cultural, and human behavioural attributes affecting the decision-making process'.[13] When applying TAA specifically to social media landscapes, one should expect additional media-specific analysis, including: historical trends, content distribution, geographical meta-data on audience provenance, quality analysis of contents, sentiment analysis, outlier performers and detection of influencers.

Despite technological capabilities, parts of the informational horizon remain unavailable to any analysis. Specifically, social media create a hardly predictable complex system of contents, users and real-world events. The D.U.N. (Defence, Uncertainty, and 'Now Media') project funded by the English Research Council studies this persistent area of uncertainty, highlighting three specific critical areas:[14]

1 Social media are inherently unpredictable and ever-mutating due to fast-paced flow between users. Consequently, this information environment 'can (continuously) reconfigure political and public perceptions'.

Hence it could be misleading to uncritically employ current or previous analyses in designing new communication strategies. Each configuration in the information landscape is unique and will reconfigure itself suddenly and unexpectedly.

2 It is possible to perform detailed analysis on the composition of social media users (demographic, behavioural, psychological, geographical, diversity or consensus of consumer attitudes). In spite of this, 'recipients and authors of social media remain unpredictable (and essentially unknowable)'.

Potential unpredictability of the audience could severely weaken the basis of a communication strategy based on a target-centric approach. The challenge here is twofold. First, acknowledging unpredictability of the informational landscape has obvious direct effects on audience selection, with an equivalent sort of unpredictability of quantity, quality or engagement of involved users. Second, the link between real-world citizens and social media users is hard to define conclusively, especially in its cause-effect relationship.

3 Military personnel have the dual nature of internet users and professionals. Their habits online and on social media pose new threats to operation security. Apparently innocuous information could be leveraged to harm or undermine the effectiveness of undertaken actions.

During preventive assessment, one's own attack surface is obviously evaluated. Still, it is essentially unknowable whether personnel successfully adhere to issued guidelines, whether they adopt unexpected ways of communicating on social media, or whether enemies discover unforeseen ways to exploit inevitable information production.

Despite the variety of preliminary analyses of the earlier doctrines, one must stress the presence of an implicit theoretical assumption: the chance to succeed in an information operation is directly proportional to the amount of information available ('more is better'). This could be schematised as follows: the best available knowledge on target A enables one to perfectly tailor themes and messages B in order to influence A and effectively achieve C. While the general risk of assuming proportional causality between knowledge and desired effects is acknowledged in the discussed doctrines, this syllogism implies another, more subtle, premise: optimising the outcome depends on maximising the amount of available information. This should be considered cautiously in light of deep uncertainty within social media and digital domains.

Planning and executing

The relationship just discussed between objectives, activity planning and execution is explicitly considered by the US JP 3-13. The line connecting operational ends, TAA and message creation is established in a chain reaction of cause and effect:

> Mapping the expected change (a theory of change) provides the clear, logical connections between activities and desired outcomes by defining intermediate steps between current situation and desired outcome and establishing points of measurement.[15]

This route should guarantee both a clear path to desired ends and different indicators to monitor and constantly adjust the execution. In addition, NATO's Bilateral Strategic Command Information Operations Reference Book describes a detailed roadmap to define strategic communication plans. It sets sequential stages, from a higher political stage down to the operational and executional stage. It follows a standard workflow: starting with assessing the information environment, it follows the definition of information objectives, themes and master messages, target audience and finally sets the actors and coordination required to execute the communication campaign. 'Themes' and 'master messages' act as guidelines in the strategic communication plan explicitly indicating do and don'ts, weaknesses or convincing points, and are designed according to the nature of the expected target audience. Themes and master messages serve as a directing force between general objectives and final implementation.

Summarising, the activities of planning and execution rely heavily on knowledge available to planners. During these stages he/she is expected to leverage both situational awareness and available assets. Nonetheless, even if an information operation will be executed in the specific domain of digital media and social network, it can still exploit various normative activities including psychological operations, deception, electronic warfare, kinetic actions and computer network operations.

After establishing complete situational awareness of the digital battlefield, the strategist proceeds in designing informational objectives, general themes and master messages. This conceptual chain serves to translate broad strategic objectives into actual messages. Every social media platform or digital arena has specific communicative dynamics and content characteristics that should be taken into account with dedicated resources.

Like these general steps, known information is decisive for successful planning and execution. These phases are nonetheless exposed to various uncertainties: communication planning strategies are ordinarily based on best practices (that may sometimes be ineffective) and execution is exposed to unforeseen instances almost by definition.

More broadly, the problem of translating complex strategical requirements into real-world effects will be easier if one splits the goal into subroutines and secondary tasks. Each resulting part should be manageable and effectively measurable. However, while local social media communication activities could be perfectly manageable and thoroughly measurable, it should be emphasised that they gain their value only as a functional part of a complex system. That is, controlling one or more social media discussions doesn't necessarily lead to mastering the overarching narration across the whole information environment.

In response to this unsolved equilibrium, Thomas Elkjer Nissen proposed replacing this top-down communication approach with a more open-ended one.[16] A cross-media communication strategy is designed to explicitly exploit uncertainty in social and digital media. That is, the fundamental strategic approach is reversed: disseminate coherent pieces of information through different channels. While themes and master messages will conserve their structural coherence, the messages are diverse and address specific audiences on different platforms. The result is an open-ended strategy, using the aforementioned 'stickiness' in order to give each and every targeted user the possibility to interact and construct their own version of the communicated message. Replacing linear storytelling, this promotes a distributed narrative where micro pieces of content are available for further integration, sharing and connecting by users. Obviously, different uncertainties emerge. Co-creation and open-ended narratives mean loosened control over development, reception and diffusion of core-messages and narratives. This could result in either narration backfire or sudden strokes of good luck. Properly adapting messages through different media requires significant

effort in developing specific strategies, templates and tones of voice. This could have significant impact on economic costs and organisational effort. Lastly, maintaining internal coherence and overarching consistency could be tougher, especially due to diversity in media employed, potential presence of adversarial activity and finally the interaction of many different operators and messages already occupying the informational landscape.

Assessment

Every communication strategist, once having implemented a plan, asks: how is it performing and is it achieving the desired effect? This raises further questions: what measurements can monitor performance? How to assess the ongoing progress of the campaign? Should one trust chosen key performance indicators and metrics for evaluating the ongoing effectiveness and forecast future tendencies?

According to US JP 3-13 doctrine, assessment never stops; it just changes its purpose, becoming part of an evaluation cycle of the strategy execution. Assessment conducts a comprehensive analysis of different procedures to assess information requirements and data collection. Monitoring capabilities are essential assets, albeit requiring continuous adjustment to dynamically adapt to analysis requirements and to evolution of the information environment. Available data are incomplete by nature and must be supplemented by the strategist's subjective insights (i.e. intuition, anecdotal evidence, past experience). The goal of monitoring is to reduce uncertainty, but this entails an essential tension: the analyst's intuition and creativity in elaborating insights from raw data could also become biased by misinterpretation or fallacious opinions.

A communication strategy: outcome optimisation

We now formulate a hypothetical social media communication strategy for a fictional case and implement it in a simple stylised way, demonstrating an outcome-optimisation approach. We consider robust-satisficing later. See Table 4.1.

The main objective of General Y is establishing himself as the dominant force within the domestic environment while creating favourable conditions to be exploited during military options. The *desired effect* has two key themes: trust among domestic public opinion, and public perception of military dominance over adversaries. *Analysis of the information environment* highlights key issues and vulnerabilities: internal stability and political tensions, broader regional positioning, main cities, cultural and religious communities, internet usage habits. This is achieved by the country assessment and the TAA, and then focusses on two different audiences: domestic citizens (neutral or favourable) and adversaries. The country assessment identifies common values: national pride in response to colonial past, religious belief,

Table 4.1 Communication Strategy

Strategic Objectives	
Situation	Country X currently involved in a tribal conflict. General Y wants to enter the conflict and affirm his power over the country
Commander's objective	General Y recognised as the main force domestically
Desired effects	Being perceived as trustworthy by citizens and potential allies Being perceived as prevailing by adversaries
Potential target audience(s)	Citizens of Country X (friendly, neutral and potential adversary) Enemies (adversary) Allies (friendly)
Potential means for achieving commander's objective	Informational assets (i.e. strategic communication, media) Military forces (i.e. security force assistance, combat operations, military information support operations, public affairs).
Potential ways (persuasive communications or coercive force)	Military actions Social media operation
Information operations	
Analysing the information environment (situational awareness, establishing baseline)	Country assessment: political, security, economic, social and infrastructure systems Target Audience Analysis
Planning and execution	Themes Master messages
Communication strategies	Assessing the results of the operation Ongoing monitoring TAA monitoring Relevant themes monitoring

desirability of modernisation. TAA involves two assessments. First, defining a baseline of reference: study of social media discussions over key themes (discussion trends, sentiment analysis and influencer involvement that could tell if, where, how and by whom some topics were discussed online). Second, specific analysis of how General Y and key leaders are perceived.

Combining objectives, desired effects and analysis of the information environment leads to the communication strategy. The strategy promotes the themes of trustworthiness and strength in two 'master messages': 'General Y is the future guide for Country X' and 'The military capability of General Y is far beyond that of any opponent'. These messages are complementary and allow development of a unique predominant narrative around General Y's actions. Since the General is trying to convince his fellow countrymen and his adversaries of his strengths, a top-down strategy should express a sense of stability while guaranteeing control of the narration.

Because we are trying to maximise the outcome, we will leverage all information to obtain optimal performance of every indicator. We want to maximise audience exposure to published messages, while maintaining maximal control over narrative creation and content spreading. Consequently, the strategy is pursued through a small number of accounts (one for General Y and one for his movement) operated only on digital platforms that guarantee optimal exposure (according to the data retrieved from the country assessment). The use of one or two accounts concentrates in a small number of places all activity of the targeted audience, maximising the interactions for every published content and thus its visibility due to high expected engagement. Also, for this reason all published content is created only in the native language, thus directly addressing the chosen audience. The campaign is designed with coherent and recognisable graphical identity across the proprietary accounts and different social media, emphasising the active presence of General Y in the informational landscape. There is consistency among contents published on different media so as to maximise the opportunity for different users to see General Y's messages. Supporters and adversaries will receive tailored messages promoted specifically for the geographical region or features identified in the dedicated TAA. Moreover, illicit assets could be considered when necessary: fake accounts could be used to foster interactions on key contents to demonstrate support and provoke social pressure on unaware citizens; organised teams of provocateurs (so-called 'trolls') could be activated against official adversarial profiles to discourage spontaneous support and influence perceptions of adversary leaders.

The ongoing assessment of proprietary channels will supply in-depth analysis of content performance (interactions, sentiment analysis) and of the audiences involved. The analysis of the campaign is used to reiterate successful messages and develop lookalike audiences by modelling potential fan-base features. The hypothesis is that if a group is already involved in something, they could also be interested in messages of another page presenting similar characteristics.

The success of the communication strategy is assessed against the growth of profile indicators (i.e. fan/followers, engagement, trend in spontaneous mentions, sentiment analysis) and the loss of interest for adversarial pages. Once a stable trend compared to the initial baseline is established, the communication strategy evolves, integrating military actions into successful narration of stability and inevitable victory.

A communication strategy: robust-satisficing

The communication strategy outlined previously is predicated on the available information and understanding being basically sound. If that assumption is correct, then top-down centrally controlled communication is a plausible approach. However, if the knowledge is fraught with error, then central control of the message will be founded on fundamental mis-understanding of the

situation and the audience; such knowledge cannot be relied on to achieve desired goals. It is one thing to deliberately use mis-information (which may be justified from a utilitarian perspective). This, however, is totally different from deliberately ignoring deep uncertainty about one's knowledge. Ignorance isn't a reliable basis for communication strategies. We return to the example of the previous section, and develop a communication strategy based on info-gap decision theory and the concept of robust-satisficing for managing deep uncertainty.[17]

The info-gap analysis of robustness uses three components: goals, knowledge and uncertainties. These are combined in assessing the robustness (to uncertainty) of a proposed strategy for achieving specified goals. Strategies are then prioritised by their robustness: more robustness is preferred over less robustness. We maximise the robustness to uncertainty, and not the quality of the outcome; the outcome will be satisfactory (though perhaps sub-optimal) over the widest range of surprise.

General Y's long-range *goals* are as before: being recognised as the dominant force in country X (prevailing over adversaries and able to assure domestic safety and order) and being trusted by the citizens. It is acknowledged, however, that deep uncertainty in our knowledge requires moderation in the rate at which goals are achieved.

The *knowledge* is also as before, based on analysing the information environment, tempered by awareness of uncertainty of that knowledge.

We now identify three elements of deep *uncertainty* in that knowledge. First, General Y is native to country X, and was raised in religious and cultural traditions that are widely observed and revered in his country. However, his career has distanced him from traditional practices, and it is unclear whether the indigenous population, which is largely rural and unexposed to foreign practices, is tolerant of General Y's secularity. Second, tribal conflict is not new to the region that today constitutes Country X. Historically, tribal conflicts have been resolved by meetings of elders in which compromise is obtained because the current balance of power is offset by recognising that the balance of power will change over time. What is unclear, however, is how much the current tribal conflicts are either subject to historical precedent or are actually instigated and exacerbated by external insurgents who are acting outside the traditional norms of tribal conflict. Finally, the concept of central authority conflicts with the traditional tribal structure of the society. It is highly uncertain that tribal leaders and their followers would accept or even believe centrally controlled and distributed information.

We will consider two alternative communication strategies: the centralised top-down strategy outlined previously, and a dispersed bottom-up strategy that is different in its conception. A strategy is highly robust to uncertainty if it achieves specified goals over a wide range of deviation of reality from our current best understanding. Conversely, a strategy has low robustness, and is highly vulnerable to uncertainty, if even small error in

our knowledge can lead to failure of the campaign to achieve specified goals. The top-down strategy has low robustness because realisation of any of the three categories of uncertainty could significantly weaken or undermine the strategy's success: General Y's secularity could readily discredit his claim to power; external instigators would not forego tribal conflict for the sake of future coexistence; the idea of central control is anathema to traditional views. The bottom-up strategy, while not guaranteed to succeed, has far greater robustness to uncertainty as now explained.

Our goal is to steadily improve the outcome of the communication campaign (promoting General Y's image), while recognising that our understanding is deficient. Audience exposure to published messages is achieved through widespread local provision of General Y's narrative, where possible in a covert or unofficial manner. Sympathetic local actors are encouraged to initiate media dialog through numerous sites and media. What constitutes 'encouragement' might not meet all the standards of civil discourse in liberal Western democracies. Also, many sites might be covertly government-owned or supported. However, the appearance, if not always the reality, is of voluntary dispersed dialogue and bottom-up communication, rather than top-down centralisation. Publication in the native language is encouraged, while not excluding foreign language publication, thereby encouraging support by international diaspora communities whose members are not all fluent in the mother tongue. While substantive coherence of the message and graphical similarity of the medium are sought, diversity is also pursued in support of the pluralistic multi-tribal image of grass-roots communication in support of General Y. Messages tailored to distinct communities are nurtured in the communities themselves, avoiding the appearance of an external source of the message. In short, while General Y is front-and-centre in the communication message, the image is of up-welling indigenous tribal support, dispersed widely over the population. General Y is, as it were, more an image or an idea than an independent and autonomous power. While current knowledge is likely wrong in all three categories of uncertainty, the bottom-up communication strategy is largely immune to these uncertainties. General Y is portrayed as realising local aspiration, the preference of tribal leaders, the fruit of local effort, the choice of the people and their tribes.

Reflections

Sometimes uncertainties are adequately managed through a straightforward top-down strategy. This holds true when the information landscape is fairly well defined and effectively understood, modelled and moulded. For example, in April 2019 General Haftar entered the Libyan conflict by spreading through its social media channels spectacular images of columns of army vehicles filmed with drones. Those videos communicated his message of strength extremely effectively and were immediately shared by all Western news agencies to concisely portray the conflict. Haftar

successfully exploited the information environment to create a perception that became a reality, at least temporarily. Through social media with global diffusion, and foreign media eager for direct sources, Haftar established a basic narrative: 'Haftar is coming and is well equipped and organized'. This situation is characterised by low uncertainty and highly predictable variables. Other situations resemble the hypothetical example of General Y, fraught with deep uncertainty about human behaviour and about complex methods and mechanisms. Such situations are fundamentally obscure and unpredictable. When can uncertainty be managed and when can it not? It is unhelpful to say that 'deep uncertainty cannot be managed; shallow uncertainty can'. The problem is that the depth of uncertainty is often what we don't know, like the depth of a muddy pool. If we can confidently specify what is unknown – the precise number of enemy tanks or the degree of our own morale – then innovation, skill and a healthy dose of luck can manage pending surprises. But if the character of the unknowns is itself hidden – innovations not yet achieved, ideological motivations not yet perceived – then preparation for surprise is far more challenging. Deep uncertainty is implausible, impenetrable and potentially very surprising. In short, we often don't know if we face deep or shallow uncertainty.

Error in designing a communication strategy can result from misjudgement of the depth of uncertainty. 'The pen is mightier than the sword', wrote Edward Bulwer-Lytton (1839).[18] Similarly, Sun Tzu declared that 'to subdue the enemy without fighting is the acme of skill'.[19] The pen is powerful, but its effectiveness depends on careful planning and close attention to managing uncertainty. Knowledge is power, but erroneous knowledge is deceptive and can lead to precipitous failure. Confidence in the power of one's knowledge is strengthened by enhancing one's robustness to surprise, because the substance of the next surprise cannot, by definition, be anticipated.

Notes

1 Ivana Marková, 'Persuasion and Social Psychology', *Diogenes* 55:1 (2008), 42.
2 Luciano Floridi, *The Onlife Manifesto* (Internet resource: Springer-Verlag GmbH, 2015).
3 Lawrence Freedman, 'On War and Choice', *The National Interest* 107 (2010), 9–16.
4 Alexus G. Grynkewich, 'Introducing Information as a Joint Function', *Joint Force Quarterly* 89 (2018), 6–7, Scott K. Thomson and E. Paul Christopher, 'Paradigm Change Operational Art and the Information Joint Function', *Joint Force Quarterly* 89 (2018), 8–15, Paul Watzlawick, *An Anthology of Human Communication. Text and Tape* (Palo Alto, CA: Science and Behaviour Books, 1964).
5 Joint Chiefs of Staff, *Joint Doctrine for Information Operations (JP3-13)* (Washington, DC: Joint Chiefs of Staff, 2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, 18.
6 Catherine A. Theohary, *Defense Primer: Information Operations* (Washington, DC: Congressional Research Service, 2018), https://fas.org/sgp/crs/natsec/IF10771.pdf, 1.

7 NATO, *Allied Joint Doctrine for Information Operations (AJP 3-13)* (Brussels: NATO, 2009).
8 Deirdre Collings and Rafal Rohozinski, *Bullets and Blogs: New Media and the Warfighter: an Analytical Synthesis and Workshop Report* (Carlisle: Center for Strategic Leadership, U.S. Army War College, 2009).
9 David Kilcullen, *Complex Warfighting: Australian Army Future Land Operational Concept (FLOC)* (Canberra: Directorate of Future Land Warfare – Australian Army, 2004), Sean Lawson, *Nonlinear Science And Warfare: Chaos, Complexity and the U.S. Military in the Information Age* (Milton Park: Routledge, 2018).
10 I.e.: informational cascade, echo chamber and filter bubble. See Soroush Vosoughi, Deb Roy, and Sinan Aral, 'The Spread of True and False News Online', *Science* 359:6380 (2018), 1146–1151, Michela Del Vicario, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley, and Walter Quattrociocchi, 'The Spreading of Misinformation Online', *Proc. National Academy Sciences,* 113:3 (2016), 554–559.
11 Collings and Rohozinski, *Bullets and Blogs*, 25.
12 Joint Doctrine and Concepts Centre (JDCC), *Information Operations-Joint Warfare Publication (JWP) 3-80* (Shrivenham: JDCC, 2002), 18.
13 NATO Bilateral Strategic Command, *Information Operations Reference Book* (Mons & Norfolk: NATO, 2010), 20.
14 DUN Project, 'The DUN Project: Defence, Uncertainty and "Now Media": Mapping Social Media in Strategic Communications, What Is the DUN Project?', *Dun Project*, 2019, http://www.dunproject.org/what-is-the-dun-project-2/.
15 Joint Chiefs of Staff, JP3-13, 66.
16 Thomas Elkjer Nissen, *#TheWeaponizationOfSocialMedia: Characteristics_of_Contemporary_Conflicts* (Copenhagen: Royal Danish Defence College, 2015).
17 Yakov Ben-Haim, *Info-Gap Decision Theory: Decisions under Severe Uncertainty* (New York: Academic Press, 2006), Yakov Ben-Haim, *Dilemmas of Wonderland: Decisions in the Age of Innovation* (Oxford: Oxford University Press, 2018).
18 Edward Bulwer-Lytton, *Richelieu; Or the Conspiracy: A Play in Five Acts* (London: Saunders & Otley, 1839).
19 Sun Tzu, *The Art of War,* Samuel B. Griffith, trans. (Oxford: Oxford University Press, 1963), chapter III, art. 3.

References

Ben-Haim, Yakov, *Dilemmas of Wonderland: Decisions in the Age of Innovation* (Oxford: Oxford University Press, 2018).

Ben-Haim, Yakov, *Info-Gap Decision Theory: Decisions under Severe Uncertainty* (New York: Academic Press, 2006).

Bulwer-Lytton, Edward, *Richelieu; Or the Conspiracy: A Play in Five Acts* (London: Saunders & Otley, 1839).

Collings, Deirdre, and Rohozinski, Rafal, *Bullets and Blogs: New Media and the Warfighter: an Analytical Synthesis and Workshop Report* (Carlisle: Center for Strategic Leadership, U.S. Army War College, 2009).

Del Vicario, Michela, Bessi, Alessandro, Zollo, Fabiana, Petroni, Fabio, Scala, Antonio, Caldarelli, Guido, Stanley, H. Eugene, and Quattrociocchi, Walter, 'The Spreading of Misinformation Online', *Proceedings of National Academy Sciences,* 113:3 (2016), 554–559.

DUN Project, 'The DUN Project: Defence, Uncertainty and "Now Media": Mapping Social Media In Strategic Communications, What Is the DUN Project?', *Dun Project*, 2019, http://www.dunproject.org/what-is-the-dun-project-2/.

Floridi, Luciano, *The Onlife Manifesto* (Internet resource: Springer-Verlag GmbH, 2015).

Freedman, Lawrence, 'On War and Choice', *The National Interest* 107 (2010), 9–16.

Grynkewich, Alexus G., 'Introducing Information as a Joint Function', *Joint Force Quarterly* 89 (2018), 6–7.

Joint Chiefs of Staff, *Joint Doctrine for Information Operations (JP3–13)* (Washington, DC: Joint Chiefs of Staff, 2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

Joint Doctrine and Concepts Centre (JDCC), *Information Operations-Joint Warfare Publication (JWP) 3–80* (Shrivenham: JDCC, 2002).

Kilcullen, David, *Complex Warfighting: Australian Army Future Land Operational Concept (FLOC)* (Canberra, Directorate of Future Land Warfare – Australian Army, 2004).

Lawson, Sean, *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age* (Milton Park: Routledge, 2018).

Marková, Ivana, 'Persuasion and Propaganda', *Diogenes* 55:1 (2008), 37–51.

NATO, *Allied Joint Doctrine for Information Operations (AJP 3–13)* (Brussels: NATO, Brussels, 2009).

NATO Bilateral Strategic Command, *Information Operations Reference Book* (Mons & Norfolk: NATO, 2010).

Nissen, Thomas Elkjer, *#TheWeaponizationOfSocialMedia: Characteristics_of_Contemporary_Conflicts* (Copenhagen: Royal Danish Defence College, 2015).

Sun Tzu, *The Art of War*, Samuel B. Griffith, trans. (Oxford: Oxford University Press, 1963).

Theohary, Catherine A., *Defense Primer: Information Operations* (Washington, DC: Congressional Research Service, 2018), https://fas.org/sgp/crs/natsec/IF10771.pdf.

Thomson, Scott K., and Paul, Christopher E., 'Paradigm Change Operational Art and the Information Joint Function', *Joint Force Quarterly,* 89 (2018), 8–15.

Vosoughi, Soroush, Roy, Deb, and Aral, Sinan, 'The Spread of True and False News Online', *Science* 359:6380 (2018), 1146–1151.

Watzlawick, Paul, *An Anthology of Human Communication. Text and Tape* (Palo Alto, CA: Science and Behaviour Books, 1964).

5 Control from the ground up

Embedding influence activities in the conduct of war

Rick Breekveldt and Martijn Kitzen

Introduction

Modern conflicts, while being fought locally, might have a far wider and even global impact. Typically, the contemporary conflict environment, or 'conflict ecosystem', consists of a wide variety of (internationally) interconnected actors and spill-over effects such as displaced persons and refugees.[1] Fall simply used the overarching term 'doctrine' for the variegated ideology, religion, belief, socioeconomic, political or other notions these wars are fought for.[2] What stands out in all these matters is the centrality of humans and their convictions, attitudes, beliefs, aspirations, norms, emotions and – most importantly – their behaviour. Despite the impact of innovations in areas such as technology and artificial intelligence, modern conflict dynamics will largely evolve as a consequence of actions undertaken in the human domain. Mitigating today's sophisticated threats, thus, requires us to look beyond the traditional military realm and inherently involves concepts focused on relevant populations.[3] Kilcullen, in this regard, devised a theory of competitive control. Based on insights from the fields of counter-insurgency and rebel governance, he argues that when armed actors vie for control over a populace, the actor 'best able to establish a predictable, consistent, and wide-spectrum normative system of control' will prevail.[4] This chapter explores this argument and proposes multiple alterations for embedding it in modern warfare. While underlining the relevance of a local perspective and human behaviour, we aim to broaden the scope of targeted actors and argue that targeting groups is more relevant than targeting individuals. For this purpose, we adopt the fundamental proposition that a competition for control can be won by altering an existing normative system instead of establishing a new system. This will enable us to build a comprehensive framework for designing influence activities rooted in actual human behaviour – contrary to focusing on attitudes, preferences, or legitimacy.[5]

Thus, this chapter not only aims to provide an academic analysis of the utility of the theory of competitive control in modern warfare but also presents a guideline for actually operationalising this population-centric approach in the conduct of war. Whereas the first decade of the

21st century saw a return of counterinsurgency and affiliated influence activities during operations in Iraq and Afghanistan, interest in this approach quickly faded away during the 2010s. This was the consequence not only of the lack of success in both wars but also of the renewed emergence of big power competition which acted as a catalyst for a reorientation toward conventional warfare. Yet, as aforementioned, the human domain remained central to the conflicts that were fought over the last decade. State actors like Russia or Iran actively exploited social cleavages in neighbouring countries, while non-state actors such as the Islamic State, Boko Haram and Al Shabab successfully established influence and control over relevant populations. Embedding influence activities in the conduct of war, therefore, is not only highly relevant for modern warfare but also essential for winning the competition for control over the local population in a conflict ecosystem. For this purpose, we will elaborate upon the theory of competitive control and subsequently develop a framework for influence activities. Doing so, however, first requires us to explore the most fundamental aspects of human behaviour and the relevance of the local level under conflict conditions.

The primacy of behaviour and the imperative of the local level

Human interaction and behaviour are central to understanding conflict. The emphasis of conflict studies however lies on attitudes and preferences of relevant populations.[6] Whereas behaviour is often influenced by interrelated concepts such as attitudes, values and norms, it is certainly not determined by these factors. Hence, emphasising attitude exclusively is insufficient.[7]

This is easily understood through the following example of an information operations (IO)-campaign in Afghanistan that aimed to reduce the number of IED-strikes and American deaths.[8] Although this effort positively changed the local attitude towards US soldiers by portraying them as friendly people devoted to their family, an increase in IED-strikes nevertheless occurred. This prompted the IO-campaign team to evaluate its methods, which revealed two reasons for the failure. First, it was found that those involved in placing the IEDs were mostly extremists, whose attitude nor behaviour could be changed. Second, and more important, the IO-campaign showed images of soldiers with their families at home, which also depicted the beauty and richness of the United States. The unintended effect of this was that the people involved in producing and transporting IEDs, who were mainly motivated by financial reasons (and therefore more susceptible to the IO-campaign than extremists), stepped up their effort in order to earn money for immigration to the United States. Thus, contrary to the desired effect, the locals involved boosted production and transportation which resulted in an abundance of available IEDs. This contributed directly to an increase in US combat deaths.

This example illustrates an assumption that attitude alone could determine behaviour, while in reality a bias towards attitude might have an adverse effect on the desired change of behaviour. Tatham, Mackay and Rowland, therefore, advocate that behaviour is what matters most in communication efforts and influencing a target audience should be grounded in social and behavioural science.[9] The term communication, in this regard, not only concerns verbal communication, but *all activities* aimed at influencing the *behaviour* of an actor.

Since behaviour is key, it is relevant to explore this concept further. Clearly, all humans differ. At the individual level, biological, psychological and neurological variations lead to immense differences in outlook and behaviour. This is further augmented by *inter alia* sociological, geographical and climatological differences at group level. These differentiations will lead to significant variety in behaviour. In addition, different normative standards will lead to a different appreciation of behaviour and actions. In other words, what may be considered unacceptable at a certain place or a certain point in time may be customary and widely accepted at another place or another moment.

Consequently, behaviour should always be understood from a local and temporal perspective. This, however, is more complicated than it seems. Bar-Yam, in this regard, emphasises that the complexity of the human civilisational system, combined with progressive specialisation, blurs our ability to understand society as a whole and only enables us to understand a small portion of our social environment.[10] Applied to contemporary conflicts, this insight implies that any attempt to define and understand concepts such as legitimacy and extremism should be understood from a temporal, *local* behavioural context. This is echoed in the debate on legitimation in both counterinsurgency and rebel governance literature, which stresses that lasting effects can only be obtained by exploiting local patterns of legitimacy.[11] The same 'local logic' pertains to extremism which can be defined as the level of deviation of the median popular preferences and therefore should also be understood from a local perspective.[12] Consequently, influencing behaviour as part of the conduct of war requires the ability to tailor all relevant activities to local circumstances. How to design and implement such an approach?

Discussions on how to enhance popular support through legitimation are often dichotomised in top-down or bottom-up approaches.[13] Another way to categorise these approaches as strategies can be provided by the owners of the problem, the internal actors, or by external actors who intervene. In this view, the top-down approach is often supported or conducted by external actors. Typically, the lack of a proper understanding of the situation forms a major problem for the intervening actor. Christia, for instance, describes in detail the continuously shifting 'intergroup alliances in multiparty conflicts' in Afghanistan, Iraq and Bosnia. Kitzen refers to the same dynamic of local leaders in contemporary Afghan tribal

society.[14] These shifting alliances eventually lead to interveners having supported their own foes, and both authors show that these 'alliances' are actually based on local leaders' self-interest and opportunism. 'Alliance'-labels, therefore, might be hardly useful and probably irrelevant at the local level, and only make sense as part of an 'externally imposed construct' – what sociologists and anthropologist term an etic framework.[15] This is the opposite of the bottom-up, local, perspective incorporating the view of the problem-owners – better known as 'emic' –, which greatly enhances understanding of the local situation.[16] Moreover, such an approach also fosters collaboration with the local populace, and allows for identification and achieving of locally attainable goals. However, this is not to say that a local perspective is the solution to all problems. Kilcullen explains the necessity to strike a balance between both an external and internal actor-driven approach: to avoid fetishising external, technocratic, top-down, white-guy-with-clipboard knowledge. At the same time, it also tries to avoid the magical thinking associated with treating local people as the fount of all knowledge and insight. If locals could understand and agree on the problem, let alone fix it, there'd be no need for outside intervention. If outsiders understood and could fix the problem, their interventions wouldn't be failing so often. Both outsiders and locals need to come together, in defined spheres of expertise and in a defined process, to jointly design approaches to the problem.[17]

Thus, co-designing an acceptable solution from both internal and external perspectives provides a solution for enhancing popular support and bolstering the position of a local government. This might have far reaching consequences as the local perspective of success, which can only be understood in emic terms, should inform an external actor's political choices and strategy.[18] Bar-Yam supports this as he underlines the necessity of involving people within any complex civilisation-system and stresses the relevance of analysing the complexity and scale of necessary behaviour to counter internal and external challenges.[19] In line with the importance of humans in conflict and the primacy of behaviour, both local and political notions of success should not only be defined as measurable, realistic and attainable objectives, but should take account of localised human behaviour.

Competitive control

Building an influencing framework also requires exploring the utility of the theory of competitive control in the conduct of modern war. Kilcullen has based his theory on the work of, among others, Fall, who, debating the Vietnam War, explained that 'any sound revolutionary warfare operator … most of the time used small-war tactics – not to destroy …, of which they were thoroughly incapable, but to establish a competitive system of control over the population'.[20] In this regard, the 'military aspect' is only the supporting effort, while the political, administrative and ideological aspects are

the primary efforts 'to the furtherance of an ideology or a political system'. Kilcullen has expanded upon this view of competitive control:

> In irregular conflicts …, the local armed actor that a given population perceives as best able to establish a predictable, consistent, and wide-spectrum normative system of control is most likely to dominate that population and its residential areas. Simply put, the idea is that populations respond to a predictable, ordered, normative system that tells them exactly what they need to do, and not do, in order to be safe.[21]

This theory, however, can be challenged. Most fundamentally, it is criticised for assuming that, in order to compete for control, actors have to 'establish' a normative system. We start from this position and note that rather than creating a *new* normative system, there is already 'some set of [local] activities' in place, which forms the actual object of competition.[22] Thus, there is no requirement to establish a new system. Actors might instead aim to alter the existing local normative system to their advantage.

The key mechanism underlying the concept of competitive control is the prevalence of predictability and consistency over the content of a rule-set for enforcing the normative system.[23] Kilcullen explains that consistently enforcing the publicly known rule-set leads to a perception of safety and 'allows a normative system to function'. The distance between the preferences of the actors and the *policies enacted* – and not the ideological position itself – is the issue at stake.[24] While rebels have a vested interest in aspiring for their ideal doctrine, they will, if necessary, adopt a pragmatic approach and enact policies closer to civilian preferences to enlarge popular support, making ideological distance a tool to influence a population. The premise here is that it is not merely the 'doctrinal' position or distance that matters; it is the enactment of its divergence from the popular median that is most relevant. Yet again, it is tangible behaviour that matters most.

When we seek to study the way behaviour can be influenced as part of the conduct of war, it is also important to stress that 'control' should not be mistaken with 'imposing order through unquestioned dominance'. Instead it boils down to 'achieving collaboration towards a set of share objectives'.[25] Whereas non-state opponents might adopt an approach of establishing control through coercion, Western-type state actors typically favour more persuasive actions such as provision of essential services and effective legislation.[26] In both cases, however, control can be understood as the ability to influence the behaviour of the relevant population(s). This offers a first point for expanding this theory as today's complicated conflicts are typified by the involvement of a myriad of actors, both state and non-state. The question, therefore, is whom exactly to control in order to obtain success in modern warfare.

The primary actors in any conflict ecosystem are the forces of the governing authorities and the challengers who are vying for power, but also the population. Traditionally, the struggle for control is conceptualised as

a contest between the former two *over* the population. As such, this latter category is implicitly denied agency. This, however, is far off from reality as civilians themselves employ different 'survival strategies' such as fleeing, passivity, armed neutrality, supporting one actor, periodically switching sides or simultaneously supporting all sides in the contest for control.[27] Moreover, people also hold an interest in the level of control of their 'rulers', aspire for a degree of self-determination and self-rule and are, for instance, consciously interested in the 'doctrine' that governs daily life.[28] The struggle for control therefore is a highly dynamic three way affair that also involves the relevant population. These actors, their interrelationship and the context are visualised in Figure 5.1. The 'control'-dot indicates the level of control per objective an actor aims to achieve. Indeed, all three actors are to some extent capable of influencing the level of control. Considering the population as passive bystanders, therefore, will lead to a flawed understanding. A binary interpretation of the competition for control, thus, ignores the intricacies of the social system as a whole.

It should be noted that the three primary actors in our model each are far from homogeneous. Authorities typically consist of governments and supporting intervening states, populations often reflect the fragmented character of a conflict society and often more than one rebel group is competing for influence. Another, related, feature of the contemporary security environment

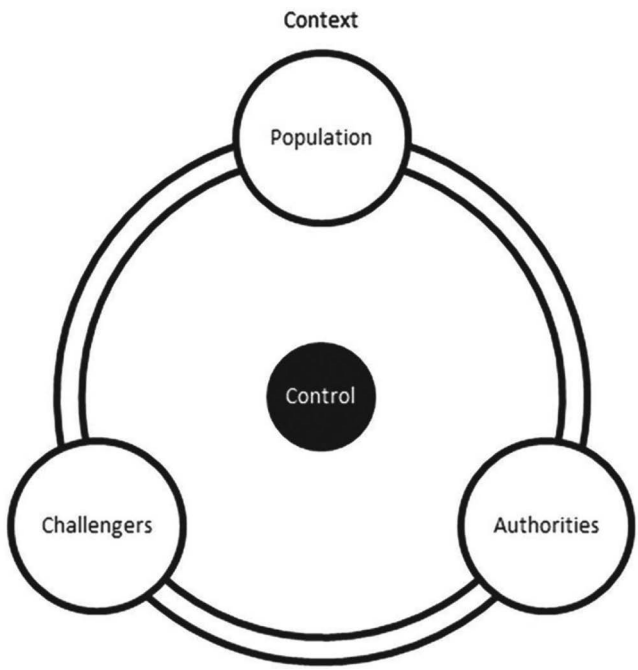

Figure 5.1 Actor/Control Model

is that conflicts are rarely isolated events. Instead, contextual factors such as foreign or transnational support frequently form the background of the dynamical contest for control. This is further complicated by the support which comes from different foreign actors and agencies, each of whom may have competing objectives.[29] Thus, the modern conflict ecosystem reflects a mosaic of different actors that interact with each other and with external influences. This indicates there is no 'one level of control': the extent of control an actor exerts might differ per objective the actor aims to achieve. A government might be able to influence people to register as voters, but may be completely unable to persuade them to provide intelligence on insurgent activities. Therefore, it is necessary to distinguish between different objectives and required level of control, and determine appropriate influence strategies. Without playing down the complexity of modern conflicts, the proposed three-actor model offers a first step for understanding this highly dynamic competition as it can be applied per objective, with the 'control'-dot (Figure 5.1) visualising the current and desired situation. Our model offers a first indication of which actor(s) should be influenced in order to obtain the sought-after effect.

How to put this into action? First it is important to discuss the question of how exactly influencing works. Human decision making is considered to be 'rational', that is, based on a cost-benefit calculus.[30] Behavioural studies, like Kahneman, remind us that decisions and choices are affected by different factors and limitations such as time and a sense of crisis.[31] These factors affect one's ability to formulate and execute logical strategies as well as the understanding of actions and the consequent counterreactions of others.[32] When applied to modern warfare this may lead to diverging conclusions: either to a simplification bias, with actors expecting logically derived results of another actor's cost-benefit calculus or to the conviction that targeting behaviour is too difficult and will lead to unpredictable effects.[33] Furthermore, there is also the question whether or not all actors in a system are influenceable. Deterrence theory, for instance, considers influencing terrorists troublesome.[34] While, indeed, some actors might be so (un)supportive of a doctrine that they will probably not alter their behaviour, the vast majority of people are influenceable (see Figure 5.2). There might be a percentage of 'irreconcilables', whose convictions are unalterable and whose behaviour cannot be influenced. These extremes, however, are rare, and even die-hard true believing terrorists are often influenceable.[35]

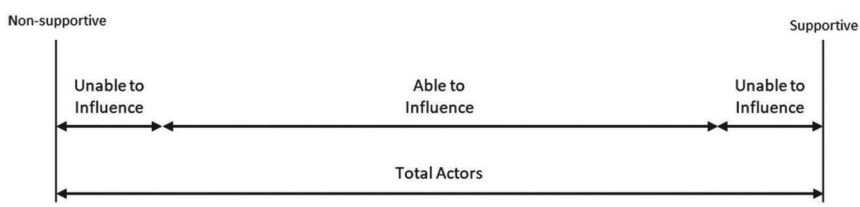

Figure 5.2 Ability to Influence Actors[36]

An individual's behaviour is difficult to predict. As a social species, humans in a group are targetable and amendable for change. Defining and distinguishing groups is often oversimplified and as such either irrelevant or incorrect. Complexity theory offers help for overcoming this problem and advances the understanding of relevant groups.[37] When a subgroup of a complex system has coordinated behaviour, or simply put, when 'members' of a single defined group within the system act in a similar vein when confronted with the same specific impulses, the group has been defined correctly. A well-defined group, therefore, is better understandable and influenceable than an individual.[38]

It is important to keep the context in mind and analyse a group on the right level. A lack of nuance in dichotomising groups typically leads to incorrect conclusions about peoples' behaviour. The specific facts on the ground influence the behaviour of the population. For instance, even under the rigid self-proclaimed Islamic State-regime, there were enormous differences in behaviour and survival strategies between fighting age males who recently lost their wives and family and married fighting age males who believed in their ability to keep their relatives safe. This shows the relevance of properly vetting groups and their specifics.[39] It also demonstrates that the social spectrum as a whole should be understood in a nuanced and deliberate way. Identifying and segmenting relevant groups, therefore, is a highly difficult process which needs to be done to correctly identify attainable behavioural aims.

To summarise, it is important to note that we have identified three alterations to the theory of competitive control. First, instead of establishing a new normative system of governance, altering the existing system is a more likely approach. Second, we highlight a three-actor model. This means that authorities should include both challenger(s) and population when imposing a normative system, while also considering their own role and (biased) understanding. Third, we found that an actionable approach should focus on changing the visible and tangible behaviour of actors by influencing relevant groups that need to be purposely identified. This of course requires a thorough understanding of local dynamics, which is intimately related to the aforementioned premise of co-design. Let us now discuss a framework for embedding this in the conduct of war.

A framework for embedding influence activities in the conduct of war

Influencing encompasses employing activities that are part of a spectrum varying from persuasion to annihilation for either directly or indirectly addressing relevant actors. In case of a competition for control, contesters apply 'a range of capabilities across a spectrum from persuasion through administration to coercion, and they are designed by armed actors – owners or proponents of the system – as a mean to corral, control, manipulate,

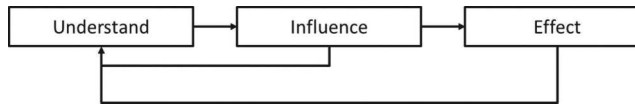

Figure 5.3 Proposed Understand, Influence and Effect Framework

and mobilize a population'.[40] However, as mentioned, this first requires actors to understand the problem and those involved and formulate realistic objectives. While a framework is helpful for operationalising this approach, it should be emphasised that any concept is a guide. Yet, this provides utility for realising the desired level of control. In its simplest form our proposed framework encompasses three interrelated stages comprising understand, influence and effect (Figure 5.3).[41] This represents a conceptual approach of an actor's process of influencing the actual outcome of a situation (which can be visualised by repositioning the 'control-dot' in Figure 5.1). While these three stages might appear blatantly obvious, influence activities often take place without properly defining the (non-)desired and attainable effects or without an appropriate understanding of the situation.

The process itself is, of course, debatable and apparent critique on the linear projection of these steps need to be addressed directly, because it depicts a highly simplified concept of reality. The perpetual changing actors, their interests, circumstances, continuous learning, actions and counterreactions will never be reflected by such a simplified process. However, this model provides a clear analytical framework to start with. Let us now first turn to its different stages.

To understand violent conflicts and to help realise solutions etic and top-down perspectives remain relevant. This may include open source analysis and other research conducted by for instance intelligence services and think-tanks. Such research should focus on attainable behavioural change of the population and challengers to achieve the desired solutions. Emic and local-level understanding of the situation are, however, essential to achieve lasting solutions. Micro-level analysis according to anthropological and sociological research protocols helps to understand the emic perspective.[42] The outcomes should be broadened by incorporating the insights of local residents, who bring a micro-level understanding of their own environment. This *ground truth* understanding can be achieved through for instance community policing or deploying special operations forces, who traditionally focus on intelligence-collection and forging local partnerships. Consequently, local and bottom-up perspectives should be coupled – or co-designed – with etic and top-down perspectives which will aid in formulating broader spectrum solutions and will also place these solutions within a wider context.

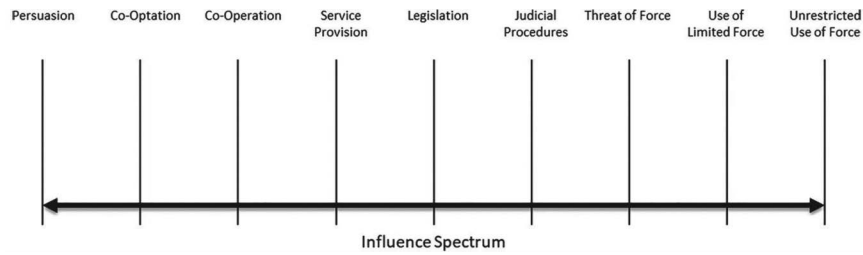

Figure 5.4 Influence Spectrum

While not aiming to describe all possibilities for influencing an actor, it should be noted that the suggested approach is most inclusive.[43] On the one end of the influence-spectrum (Figure 5.4) one will find consensual strategies such as persuasion, co-optation and cooperation. In the middle, one will find administrative strategies such as legislation, service provision and judicial or legal procedures. On the other end of the spectrum, one will find the threat or use of force, including targeting and decapitation strategies.

There is significant overlap, interrelationship and reciprocity between all these concepts. Furthermore, the activities can be further subdivided as persuasion, for instance, might involve incentives, inducements, reassurances or other positive reinforcement measures. The framework thus incorporates all available influence options and aims to broaden the spectrum of target groups to include segments of the authorities, the challengers and the population. This also opens the way for practices traditionally associated with interstate conflicts to be applied more widely; the broadest possible spectrum of activities should be contemplated to achieve the desired effects. For instance, although coercive diplomacy is developed for state interaction, it should not be dismissed as a feasible strategy against non-state actors.[44] Last, all activities should be aimed at influencing the local level, while also incorporated in the political-level strategy. This is distinct from current practice, in which political interests exclusively dictate activities on the ground and sometimes even hamper successful conduct of activities.[45]

To make the theoretical persuasion-coercion spectrum practically applicable it is relevant to define what the objectives are and how these can be achieved. Conceptions of desired effects matter and too simplistic and externally composed notions such as 'a safe and secure environment' or 'stability' are problematic in the practical reality on the ground. Kilcullen emphasises an emic perspective, and underlines the necessity of 'a constant realization that outsiders *don't* understand how things work, and therefore need to experiment, test hypotheses, start off small, and seek local context'. Furthermore, when aiming

to influence particular actors to achieve desired effects, then there should be methods to understand the efficacy of influencing. Measuring desired and non-desired effects, therefore, should be based on (quantifiable) behavioural outcomes and focus should be less on the current practice of measurement of performance such as measuring how many operations have been conducted or measuring how many insurgents have been killed or detained.

Putting this framework to practice requires integration from the onset of a mission. Hence co-designing is not only instrumental in establishing a profound understanding and identifying the right effects as well as methods for measuring them, it is also highly important for the sake of embedding influence activities in the conduct of war. But how to make sense of such a complicated task and start co-designing?

Understanding the level of control is a first step which can be specified by defining the different 'avenues' or 'lines' of conflict. Fisher and Mercado propose the use of the United Nations Development Programme's 16 areas of governance as a starting point for defining the 'lines of conflict' and 'lines of control', possibly in conjunction with the 'lines of effort' as detailed in Field Manual 3-24 Counterinsurgency.[46] RAND, in its seminal work Paths to Victory, has conducted a review of nearly 300 factors of influence on 70 counterinsurgency case-studies and, using both qualitative and quantitative analysis, identified the 26 most relevant effects to achieve or avoid for success in counterinsurgency. Using these factors could provide a useful guideline for influence activities designed to fit the local context.[47] RAND's factors are quantifiable, measurable and include various actors in the conflict ecosystem. Refining these factors into desired and non-desired behavioural outcomes can provide a solid starting point for a 'government' as this actor's *input* for the co-design phase, leading to specific and locally attainable desired outcomes based on actual behaviour.

Dissecting the desired end state into specific and measurable factors will allow for a more nuanced and precise view, and will probably contribute to addressing the problem effectively. This will also improve identification and classification of the extent to which actors have influence over a specific 'line' or 'path'. Key, however, is that this framework merely provides a starting point and that the actual strategy for influencing the behaviour of relevant segments of a society should be devised using a local, context-specific and emic perspective.

Further it is essential to grasp that there is a *degree* of control, which might differ per specific factor. While binary juxtaposition aids quantitative analysis and simplifies reporting, only qualitative nuance will lead to relevant, measurable and attainable objectives. Formulating these objectives in behavioural terms, such as 'the local population provides actionable intelligence on rebel activities', helps quantifying them and doing so will help minimise the risk of mistaking measures of performance with measures of effectiveness. A more encompassing and elaborated

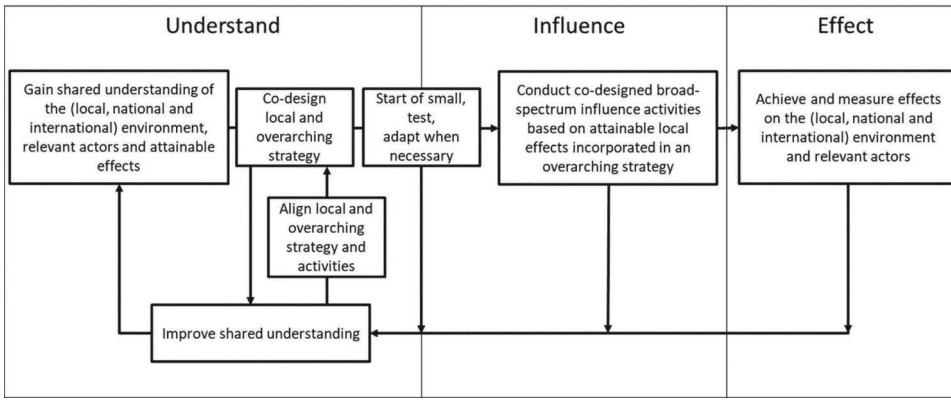
Understand
Influence
Effect
Gain shared understanding of the (local, national and international) environment, relevant actors and attainable effects
Co-design local and overarching strategy
Start of small, test, adapt when necessary
Conduct co-designed broad-spectrum influence activities based on attainable local effects incorporated in an overarching strategy
Achieve and measure effects on the (local, national and international) environment and relevant actors
Align local and overarching strategy and activities
Improve shared understanding

Figure 5.5 Elaborated Understand, Influence and Effect Framework

framework, as presented in Figure 5.5, takes the abovementioned aspects into account.

Conclusion

Humans are central to conflict and as such influencing the behaviour of relevant actors is essential. The theory of competitive control has provided us with a starting ground for embedding influence activities in the conduct of war. In our view, however, three alterations are necessary. First, there is no need to establish a new normative governance system, since there is already a normative system in place which can be altered for establishing control. Second, the scope of targeted actors should be broadened to include authorities, challengers and the population. Third, focus should be on changing actual human behaviour. This can be attained by targeting groups instead of individuals. Relevant groups should be properly defined and understood in the context of the overall conflict ecosystem.

For this approach to succeed it should be tailored to the specific local situation. Co-designing solutions and approaches, incorporating both an etic and emic perspective, combining top-down and bottom-up approaches all function to achieve a shared understanding. This provides an underpinning for defining and conducting influence activities as well as an understanding of how to interpret results and measure success. Such a localised approach also implies that local behavioural objectives, as formulated in the co-design phase, should be incorporated in the political aims of host and intervening states, which requires flexibility in the (political) strategy. In current practice, however, political guidance is rarely adjusted to context-specific results and often dictates actual activities. Instead of

rigidly sticking to overarching concepts, including (a perception of) legitimacy, it is important to adapt these concepts in such a way that they are relevant on the local level.

This chapter has presented a framework for embedding influence activities in the conduct of war. The phases understand, influence, and effect offer a clear path for deploying a full spectrum of influence activities on the basis of an appropriate understanding of the conflict ecosystem, its dynamics and the way to influence relevant groups. This, however, should always be tailored to the specific circumstances. Doing so gives the much-needed guidance for obtaining the desired effect(s). The suggested framework, therefore, should be considered a first step for enhancing existing influence activities in the conduct of war. As human behaviour will remain dominant in future conflicts population-centric concepts should be anchored and serve to sharpen thinking on war and peacemaking.

Notes

1 D.J. Kilcullen, 'Three Pillars of Counterinsurgency', *U.S. Government Counterinsurgency Conference* (Washington, DC: U.S. Department of State, 2006).
2 Bernard B. Fall, 'The Theory and Practice of Insurgency and Counterinsurgency', *Naval War College Review* 18:3 (1965), 21–38.
3 Charles T. Cleveland, Shaw S. Pick, and Stuart L. Farris, 'Shedding Light on the Gray Zone: A New Approach to Human-Centric Warfare', *Army Magazine*, 17 August 2015; S.M. D'Souza, 'Countering Insurgencies, Terrorism and Violent Extremism in South Asia', *Small Wars & Insurgencies* 28:1 (2017), 1–11; R. Thornton, 'The Changing Nature of Modern Warfare', *The RUSI Journal* 160:4 (2015), 40–48.
4 D.J. Kilcullen, *Out of the Mountains – The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013), 126.
5 Christina van Kuijck, 'Deligitimizing the Adversary: Understanding Actor and Audience Analysis as a Tool to Influence and Persuade', in Paul A.L. Ducheine and Frans P.B. Osinga, eds., *Winning Without Killing: the Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, *Netherlands Annual Review of Military Studies 2017* (The Hague: Asser, 2017); Susan Michie, Maartje M. van Stralen and Robert West, 'The Behaviour Change Wheel: A New Method for Characterising and Designing Behaviour Change Interventions', *Implementation Science* 6 (2011), 6–42.
6 Andrew J. Gawthorpe, 'All Counterinsurgency is Local: Counterinsurgency and Rebel Legitimacy', *Small Wars & Insurgencies* 28:4/5 (2017), 841.
7 Stathis N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge: Cambridge University Press, 2008), 94–104.
8 A.S. Dietz, 'Countering the Effects of IED Systems in Afghanistan: An Integral Approach', *Small Wars & Insurgencies* 22:2 (2011), 385–401; Steve Tatham, 'Address to the Netherlands Armed Forces', Roosendaal, 16 January 2017.
9 Andrew Mackay, Steve Tatham and Lee Rowland, *The Effectiveness of US Military Information Operations in Afghanistan 2001–2010: Why RAND missed the point*, Central Asia Series, Defence Academy of the United Kingdom, 2012; Steve Tatham, *Strategic Communication: A Primer*, Advanced Research and Assessment Group Report 08/28 (Defence Academy of the United Kingdom, 2008).

10 Yaneer Bar-Yam, *Complexity Rising: From Human Beings to Human Civilization, a Complexity Profile* (Cambridge: New England Complex Systems Institute, 1997), 3–33.
11 Isabelle Duyvesteyn, 'Rebels & Legitimacy; An Introduction', *Small Wars & Insurgencies* 28:4/5 (2017), 669–685; Martijn Kitzen, *The Course of Co-Option: Co-Option of Local Powerholders as a Tool for Obtaining Control over the Population in Counterinsurgency Campaigns in Weblike Societies* (Doctoral Disseration, Amsterdam University, 2016).
12 Jennifer Keister and Branislav L. Slantchev, 'Statebreakers to Statemakers: Strategies of Rebel Governance', Unpublished Manuscript (2014), http://slantchev.ucsd.edu/wp/pdf/RebelGovern-W079.pdf, 10.
13 Gawthorpe, 'All Counterinsurgency is Local', 843–848.
14 Fotini Christia, *Alliance Formation in Civil Wars* (Cambridge: Cambridge University Press, 2013), 230–242. Kitzen, *The Course of Co-Option*.
15 Kilcullen, *Out of the Mountains*; Kitzen, *The Course of Co-Option*.
16 A. Bergman and M. Lindgren, 'Navigating between an Emic and an Etic Approach in Ethnographic Research. Crucial Aspects and Strategies When Communicating Critical Results to Participants', *Ethnography & Education* 13:4 (2018), 477–489; M.W. Morris, et al., 'Views from Inside and Outside: Integrating Emic and Etic Insights about Culture and Justice Judgment', *Academy of Management Review* 24:4 (1999), 781–796.
17 Kilcullen, *Out of the Mountains*, 256.
18 Kitzen, *The Course of Co-Option*, 539–548.
19 Yaneer Bar-Yam, *Complexity Rising*, 3–32.
20 Fall, 'The Theory and Practice of Insurgency and Counterinsurgency'.
21 Kilcullen, *Out of the Mountains*, 126.
22 D. Fisher and C. Mercado, '"Competitive Control": How to Evaluate the Threats Posed by "Ungoverned Spaces"', *Small Wars Journal*, 2014.
23 Kilcullen, *Out of the Mountains*, 137–138; Michael A. Hogg and Danielle L. Blaylock, *Extremism and the Psychology of Uncertainty* (West Sussex: John Wiley & Sons, 2012); Daniel Schacter et al., *Psychology* (London: Palgrave, 2016), 323, 654.
24 Keister and Slantchev, 'Statebreakers to Statemakers'.
25 Kilcullen, 'Three Pillars of Counterinsurgency'.
26 Roland Paris and Timothy D. Sisk, *The Dilemmas of Statebuilding: Confronting the Contradictions of Postwar Peace Operations* (London and New York: Routledge, 2009).
27 Kilcullen, *Out of the Mountains*, 160–167; Joel S. Migdal, *Strong Societies and Weak States: State-Society Relations and State Capabilities in the Third World* (Princeton, NJ: Princeton University Press, 1988), 24–33, 207–236.
28 Anthony Giddens, *The Constitution of Society* (Berkeley and Los Angeles: University of California Press, 1986), 16.
29 Cedric de Coning and Karsten Friis, 'Coherence and Coordination: The Limits of the Comprehensive Approach', *Journal of International Peacekeeping* 15:1/2 (2011), 243–272.
30 Thomas Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960); Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).
31 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).
32 Robert Jervis, Ned Lebow and Janice Gross Stein, *Psychology and Deterrence* (Baltimore, MD: Johns Hopkins University Press, 1985); Keith Krausse, 'Rationality and Deterrence in Theory and Practice', in Craig A. Snyder, ed., *Contemporary Security and Strategy* (New York: Routledge, 1999), 120–149.

33 Samuel L. Popkin, *The Rational Peasant: The Political Economy of Rural Society in Vietnam* (Berkeley: University of California Press, 1979); T. David Mason, *Caught in the Crossfire: Revolutions, Repression, and the Rational Peasant* (Lanham, MD: Rowman and Littlefield Publishers, 2004); Edward U. Lorenz, 'Predictability: Does the Flap of a Butterfly's Wings in Brazil Set off a Tornado in Texas?', *Classics* 20:3 (2015), 260–263.
34 T.V. Paul, Patrick M. Morgan and James J. Wirtz, eds., *Complex Deterrence. Strategy in the Global Age* (Chicago: University of Chicago Press, 2009); A. Wenger and Wilner, eds., *Deterring Terrorism: Theory and Practice* (Stanford, CA: Stanford University Press, 2012); Micah Zenko, *Between Threats and War: U.S. Discrete Military Operations in the Post-Cold War World* (Stanford, CA: Stanford University Press, 2010).
35 Robert F. Trager and Dessislava P. Zagorcheva, 'Deterring Terrorism: It Can Be Done', *International Security* 30:3 (2006); Rick Breekveldt and Martijn W.M. Kitzen, 'Coercion and Non-State Actors: Lessons from the Philippines', *Combating Terrorism Exchange* 9:1 (2019), 13–28.
36 Adapted version of Gordon McCormick's Area of Influence Model, Naval Postgraduate School, as described by Eric P. Wendt, 'Strategic Counterinsurgency Modeling', *Special Warfare* 2005, 2–13.
37 Yaneer Bar-Yam, *Complexity Rising*, 3–33.
38 Kilcullen, *Out of the Mountains*, 127.
39 Ronald E. Rice and Charles K. Atkin, 'Public Communication Campaigns: Theoretical Principles and Practical Applications', in Jennings Bryant and Mary Beth Oliver, eds., *Media Effects – Advances in Theory and Research* (New York: Routledge, 2009), 439–440.
40 Kilcullen, *Out of the Mountains*, 167.
41 This model was developed as a command support tool, has been tested and refined, and is now in use during preparation and conduct of military activities by the Netherlands Armed Forces. Operational restrictions prevent further details being disclosed.
42 Michael Pickering and Gabriele Griffin, *Research Methods for Cultural Studies* (Edinburg: Edinburgh University Press, 2008).
43 See for a detailed explanation on how to influence behaviour of actors: Van Kuijck, 'Deligitimizing the Adversary'.
44 Keister and Slantchev, 'Statebreakers to Statemakers', 6.
45 Kitzen, *The Course of Co-Option,* 534–548; Paris and Sisk, *The Dilemmas of Statebuilding*; Elizabeth N. Saunders, *Leaders at War: How Presidents Shape Military Interventions* (Ithaca, NY and London: Cornell University Press, 2011); Erwin Van Veen and Maria Derks, 'The Deaf, the Blind and the Politician: The Troubles of Justice and Security Interventions in Fragile States', *Hague Journal on the Rule of Law: Special Issue on Security Sector Reform and Rule of Law* 4:1 (2012), 76–97.
46 Fisher and Mercado, '"Competitive Control"'.
47 C. Paul et al., *Paths to Victory: Lessons from Modern Insurgencies* (Santa Monica, CA: RAND, 2013).

References

Bar-Yam, Yaneer, *Complexity Rising: From Human Beings to Human Civilization, a Complexity Profile* (Cambridge: New England Complex Systems Institute, 1997).

Bergman, A., and Lindgren, M., 'Navigating between an Emic and an Etic Approach in Ethnographic Research. Crucial Aspects and Strategies When Communicating Critical Results to Participants', *Ethnography & Education* 13:4 (2018), 477–489.

Betts, Richard K., 'Is Strategy an Illusion', *International Security* 25:2 (2000), 5–50.
Breekveldt, Rick and Kitzen, Martijn W.M., 'Coercion and Non-State Actors: Lessons from the Philippines', *Combating Terrorism Exchange* 9:1 (2019), 13–28.
Christia, Fotini, *Alliance Formation in Civil Wars* (Cambridge: Cambridge University Press, 2013).
Cleveland, Charles T., Pick, Shaw S. and Farris, Stuart L., 'Shedding Light on the Gray Zone: A New Approach to Human-Centric Warfare', *Army Magazine*, 17 August 2015, https://www.ausa.org/articles/shedding-light-gray-zone-new-approach-human-centric-warfare, (accessed 1 September 2019).
De Coning, Cedric, and Friis, Karsten, 'Coherence and Coordination: The Limits of the Comprehensive Approach', *Journal of International Peacekeeping*, 15:1/2 (2011), 243–272.
Dietz, A.S., 'Countering the Effects of IED Systems in Afghanistan: An Integral Approach', *Small Wars & Insurgencies* 22:2 (2011), 385–340.
D'Souza, S.M., 'Countering Insurgencies, Terrorism and Violent Extremism in South Asia', *Small Wars & Insurgencies* 28:1 (2017), 1–11.
Duyvesteyn, I., 'Rebels & Legitimacy: An Introduction', *Small Wars & Insurgencies* 28:4/5 (2017), 669–685.
Fall, Bernard B., 'The Theory and Practice of Insurgency and Counterinsurgency', *Naval War College Review* 18:3 (1965), 21–38.
Fisher, D., and Mercado, C., '"Competitive Control": How to Evaluate the Threats Posed by "Ungoverned Spaces"', *Small Wars Journal* (2014), https://smallwarsjournal.com/jrnl/art/%E2%80%9Ccompetitive-control%E2%80%9D-how-to-evaluate-the-threats-posed-by-%E2%80%9Cungoverned-spaces%E2%80%9D (accessed 1 September 2019).
Gawthorpe, Andrew J., 'All Counterinsurgency is Local: Counterinsurgency and Rebel Legitimacy', *Small Wars & Insurgencies* 28:4/5 (2017), 839–852.
Giddens, Anthony, *The Constitution of Society* (Berkeley and Los Angeles: University of California Press, 1986).
Hogg, Michael A., and Blaylock, Danielle L., *Extremism and the Psychology of Uncertainty* (West Sussex: John Wiley & Sons, 2012).
Jervis, Robert, Lebow, Ned, and Gross Stein, Janice, *Psychology and Deterrence* (Baltimore, MD: Johns Hopkins University Press, 1985).
Kahneman, Daniel, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).
Kalyvas, Stathis N., *The Logic of Violence in Civil War* (Cambridge: Cambridge University Press, 2008).
Keister, Jennifer, and Slantchev, Branislav L., 'Statebreakers to Statemakers: Strategies of Rebel Governance', Unpublished Manuscript (2014), http://slantchev.ucsd.edu/wp/pdf/RebelGovern-W079.pdf, (accessed 2 September 2018).
Kilcullen, D., *Out of the Mountains – The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013).
Kilcullen, D.J., 'Three Pillars of Counterinsurgency', *U.S. Government Counterinsurgency Conference* (Washington, DC: U.S. Department of State, 2006).
Kitzen, Martijn, *The Course of Co-Option: Co-Option of Local Powerholders as a Tool for Obtaining Control over the Population in Counterinsurgency Campaigns in Weblike Societies*, Doctoral Dissertation, Amsterdam University, 2016.
Kuijck, van, Christina, 'Deligitimizing the Adversary: Understanding Actor and Audience Analysis as a Tool to Influence and Persuade', in Paul A. L. Ducheine

and Frans P. B. Osinga eds., *Winning Without Killing: the Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, *Netherlands Annual Review of Military Studies 2017* (The Hague: Asser, 2017).

Krausse, Keith, 'Rationality and Deterrence in Theory and Practice', in Craig A. Snyder ed., *Contemporary Security and Strategy* (New York: Routledge, 1999), 120–149.

Lorenz, Edward U., 'Predictability: Does the Flap of a Butterfly's Wings in Brazil Set off a Tornado in Texas?' *Classics* 20:3 (2015), 260–263.

Mackay, Andrew, Tatham, Steve and Rowland, Lee, *The Effectiveness of US Military Information Operations in Afghanistan 2001–2010: Why RAND Missed the Point* (Central Asia Series, Defence Academy of the United Kingdom, 2012).

Mason, T. David, *Caught in the Crossfire: Revolutions, Repression, and the Rational Peasant* (Lanham, MD: Rowman and Littlefield Publishers, 2004).

Michie, Susan, Van Stralen, Maartje M., and West, Robert, 'The Behaviour Change Wheel: A New Method for Characterising and Designing Behaviour Change Interventions', *Implementation Science* 6:42 (2011), 1–11.

Migdal, Joel S., *Strong Societies and Weak States: State-Society Relations and State Capabilities in the Third World* (Princeton, NJ: Princeton University Press, 1988).

Morris, M.W., et al., 'Views from Inside and Outside: Integrating EMIC and ETIC Insights about Culture and Justice Judgment', *Academy of Management Review* 24:4 (1999), 781–796.

Paris, Roland, and Sisk, Timothy D., *The Dilemmas of Statebuilding: Confronting the Contradictions of Postwar Peace Operations* (London and New York: Routledge, 2009).

Paul, C. et al., *Paths to Victory: Lessons from Modern Insurgencies* (Santa Monica, CA: RAND, 2013).

Paul, T.V., Morgan, Patrick M., and Wirtz, James J., eds., *Complex Deterrence. Strategy in the Global Age* (Chicago: University of Chicago Press, 2009).

Pickering, Michael, and Griffin, Gabrielle, *Research Methods for Cultural Studies* (Edinburg: Edinburgh University Press, 2008).

Popkin, Samuel L., *The Rational Peasant: The Political Economy of Rural Society in Vietnam* (Berkeley: University of California Press, 1979).

Rice, Ronald E., and Atkin, Charles K., 'Public Communication Campaigns: Theoretical Principles and Practical Applications', in Jennings Bryant and Mary Beth Oliver (eds.), *Media Effects – Advances in Theory and Research* (New York: Routledge, 2009), 436–468.

Saunders, Elizabeth N., *Leaders at War: How Presidents Shape Military Interventions* (Ithaca and London: Cornell University Press, 2011).

Schacter, Daniel et al., *Psychology* (London: Palgrave, 2016).

Schelling, Thomas, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

Schelling, Thomas, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960).

Strachan, Hew, 'The Lost Meaning of Strategy', *Survival* 47:3 (2005), 33–52.

Tatham, Steve, 'Address to the Netherlands Armed Forces', Roosendaal, 16 January 2017.

Tatham, Steve, *Strategic Communication: A Primer*, Advanced Research and Assessment Group Report 08/28, Defence Academy of the United Kingdom, 2008.

Thornton, R., 'The Changing Nature of Modern Warfare', *The RUSI Journal*, 160: 4 (2015), 40–48.

Trager, Robert F., and Zagorcheva, Dessislava P., 'Deterring Terrorism: It Can Be Done', *International Security* 30:3 (2006), 87–123.

Van Veen, Erwin, and Derks, Maria, 'The Deaf, the Blind and the Politician: The Troubles of Justice and Security Interventions in Fragile States', *Hague Journal on the Rule of Law: Special Issue on Security Sector Reform and Rule of Law* 4:1 (2012), 76–97.

Wendt, Eric P., 'Strategic Counterinsurgency Modeling', *Special Warfare* 18:2 (2005), 2–13.

Wenger, A., and Wilner, A., eds., *Deterring Terrorism: Theory and Practice* (Stanford, CA: Stanford University Press, 2012).

Zenko, Micah, *Between Threats and War: U.S. Discrete Military Operations in the Post-Cold War World* (Stanford, CA: Stanford University Press, 2010).

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Part III

New technologies and their impact on warfare

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

6 Humans and hardware

An exploration of blended tactical workflows using John Boyd's OODA loop

Dave Blair, Joseph O. Chapa, Scott Cuomo and Jules Hurst[1]

Introduction

In 1939, Antoine de Saint-Exupery, an early commercial aviation pioneer, wrote that, amid the rapid development of aircraft technology, 'we have perhaps driven men into the service of the machine, instead of building machinery for the service of man'.[2] Nearly a century later, we run the risk of committing the same error with artificial intelligence – driving humans into the service of a machine decision cycle instead of building systems to support a human decision cycle. This worry is particularly salient in the military context. Combat brings out the best and the worst in technology – the extreme competitive pressures of the battlefield drive a relentless pursuit of small margins of performance, and those same pressures can drive combatants to compromise judgment and accept unwise risks. Artificial intelligence and machine learning (AI/ML) systems add a layer of complexity to this timeless feature of war: the drive for a marginal advantage over one's adversary will, as before, lead to the development of systems that are increasingly able to recognize and respond to changes in the battlespace. But because AI/ML system behavior can be unpredictable, the consequences of accepting unwise risks might be even higher than in more traditional cases.

These technologies, like others before them, must be deeply enmeshed with human social sensemaking faculties. Even in terms of pure military efficacy, the value of these analytical tools is intertwined with human cognition – to apply them well, we must understand how humans and hardware should interact to make sense of the world. That is, 'we,' the humans that will employ AI/ML technologies, must understand the 'why' behind their capabilities and limitations in any given environment, not just when a manufacturer says they will or will not work. Unfortunately, the widely held distinction between an operator 'in the loop,' 'on the loop,' and 'out of the loop,' fails to account for this kind of relationship between human and machine.[3] This common conception puts the machine conceptually at the center and the human at the periphery. This conception is fundamentally flawed.

These are not merely academic concerns, nor should their analysis take place in a vacuum. Because we are active duty U.S. military officers, our

point of departure for thinking about the employment of these and other systems is the 2018 U.S. National Defense Strategy (NDS). The NDS is grounded in a powerful and clear problem statement.

Eroding U.S. military advantage vis-à-vis China and Russia undermines our ability to deter aggression and coercion in key regions. China and Russia want to undermine regional balances of power and the U.S. alliance and partnership constellation.[4]

Of all the regions across the globe, the NDS places particular emphasis on the Indo-Pacific's key maritime littoral regions – for example, the Strait of Malacca, the South China Sea, the Luzon Strait, and areas in and around the Senkaku Islands. The operational problem laid out in the NDS is one in which United States and partner nations will employ relatively small units in relatively small numbers to surveil massive swaths of blue water and littoral regions, while operating below the traditional, Western levels of war.[5] AI/ML capabilities are essential to implementing the NDS's deterrence-by-denial foundation.[6]

An important part of the solution to this operational problem will likely include systems capable of predictive logistical support, as well as others that can sift through hundreds, if not thousands, of square miles of sensor imagery while identifying adversary behavior. Finally, if a military confrontation with an adversary does become necessary, those small units must operate in degraded or denied regions of the electromagnetic spectrum. Even as we agree that AI/ML systems must play an important role in this renewed era of 'long-term, strategic competition', ethical concerns about so-called 'autonomous weapons' are important and must also be incorporated into our operating concepts.[7]

In this chapter, we develop a new conceptual approach to the relationship between humans and AI/ML systems in war by interrogating interactions between correlation and being, between machine learning and human heuristics, and between uncertainty and constraints. Our model centralizes the human decision cycle and imposes constraints on machine inputs. First, in the theoretical section, we begin by establishing a baseline model of human-machine interaction by relating performance to differing levels of complexity. For the near future, humans will outperform machines past a threshold of complexity, and machines will outperform humans in contexts of lesser complexity. We then propose three different lenses through which to view complexity and uncertainty in a combat environment. The first is John Boyd's Observe, Orient, Decide, Act (OODA) loop, a widely adopted model of tactical decision-making on the battlefield.[8] The second is Melanie Mitchell's account of stability and complexity. In the third instance, we show that both Boyd's OODA loop and Mitchell's complexity map onto the dynamic targeting 'kill chain' already familiar to many military practitioners. We then propose a model that relates the boundedness of a problem set assigned to the AI/ML system to uncertainty in the relevant phase of the OODA loop, the complexity of the environment, and the kill

chain. Finally, we articulate the relationship between effective employment of AI/ML systems and the data logistics that must support them. One way to frame our effort is that we provide a novel account of what 'meaningful human control' can mean in the context of AI/ML weapons systems.[9]

Next, we apply this model to three use cases: 'tightly bounded' problems, 'loosely bounded' problems, and 'unbounded' problems. We then briefly outline two hazard cases to demonstrate the operational and ethical implications of failing to adhere to the model.

In the final section we show that the human-centric model we propose mitigates concerns in techno-social development, ethical employment in combat contexts, and in the strategic environment facing the United States and other Western states.

Theory

In this section, we develop a new conceptual approach to military uses of AI/ML systems. We reject the cybernetic account of the human's relationship to the machine's decision loop according to which the human operator is either in, on, or out of the loop. Instead, we propose a human-centric model according to which the human operator dictates the appropriate point of application of AI/ML inputs.

Baseline model: the analytical possibilities frontier

To hypothesize about the ideal-typical relationships between humans and hardware, we build on the widely held view that humans are relatively more effective than hardware when operating at higher levels of complexity. To use the AI-human gaming race as a baseline, consider the increasing complexity from tic-tac-toe, to checkers, to chess, and finally to go. We might bound the race with 'Calvinball,' of Calvin and Hobbes fame, in which the only rule is that players must constantly make up new rules. This is a game in which humans are likely to continue to prevail for the foreseeable future.[10] By plotting performance against complexity, we translate this intuition into a notional graph (Figure 6.1). This Analytical Possibilities Frontier describes tradeoffs between relatively 'math-rich' computing machines and 'judgment-rich' humans.[11] Sensemaking for both human and machine decays under conditions of increasing complexity, but it decays more rapidly for machines. There is a threshold, therefore, to the left of which machines outperform humans and to the right of which humans outperform machines. For example, an algorithmically empowered airborne sensor might exceed human capacity to count individuals in an area, but it might struggle to recognize hostile intent in the same population – a more complex task better suited to humans.

As technology improves, the hardware curve expands, causing tasks formerly suited to human judgment to become candidates for algorithmic automation. This leads to contestation between the constituencies attached to

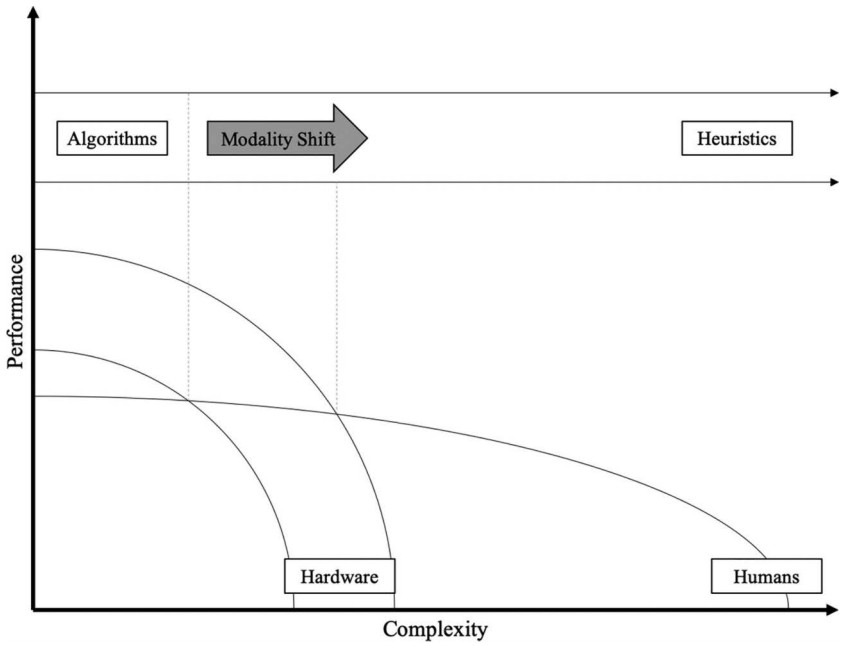

Figure 6.1 Performance-Complexity Graph

those judgment-laden tasks and the beneficiaries of automation, which leads to strategies of adoption, accommodation, and opposition between those groups. The tension is resolved in a three-step process: first, the divestiture of algorithmic tasks creates cognitive surplus.[12] Second, that surplus is re-invested in expanding the human judgment space, thereby yielding more productivity. Finally, some portion of this surplus is re-invested in maintaining the machines that run the algorithms – and in the case of military technology, in exploiting the weaknesses of the enemy algorithms. As we will show below in the first use case, this phenomenon is not unique to AI/ML and has in fact been a mainstay of decision-making in war for decades. We suggest that the AI/ML discussion is simply one more expansion of this hardware frontier, and one more re-negotiation of workflows in the wake of that expansion. One advantage of our approach, therefore, is that, though it is applicable in the immediate future, it also allows for, and even anticipates, future technological developments.

This baseline model implies that to maximize effectiveness, humans should delegate to machines those 'math-rich' tasks for which machines are ideally suited. This leaves open the question of how those tasks should be determined in the combat environment. It is to that question that we turn in the remainder of this section.

John Boyd's Observe, Orient, Decide, Act loop

John Boyd's ubiquitous OODA loop still provides value in understanding the relationship between sensing and acting in competitive environments.[13] In its simplest form, the loop begins with observation; then transitions to an orientation of the actor to the world and the set of relevant facts and tasks; then to a decision grounded in that orientation; and finally action based on that decision – which changes facts about the world and therefore requires new observation.

In Boyd's model, first derived from his dogfighting experiences and then later applied to conflict at the operational and strategic levels, two or more players both iterate through this loop to reshape the world to maximize their options and thereby improve their chances of survival. We might therefore imagine Boyd's model as fundamentally about optionality. In his paper, 'Destruction and Creation,' Boyd refers to entropy as a sense of 'foreclosed options' – knowledge or actions which have become inaccessible because the cost to access them would outweigh their benefit.[14] Accordingly, any contest is conducted across a spectrum of possible futures in which both sides (in a zero-sum game) are expanding their option space and foreclosing that of their opponent, until one player is out of options and forced to accept an undesirable conclusion.

However, there is always a third force at work above and beyond the efforts of the two contestants – chaos. While the OODA loop tries to resolve uncertain environments into frames that enable meaningful action, iterating through the loop itself generates uncertainty, especially in a contest with an adversary doing the same. The level of that uncertainty bounds the speed with which one can iterate through the loop without 'getting in front of one's headlights,' or making decisions with little ability to anticipate their outcomes.

Since the OODA loop itself begins in conditions of relative uncertainty, clarifying with each step toward action, higher environmental levels of uncertainty will affect each step in the loop differently. More complex environments will require more deliberate bounding, more assumptions, and more heuristic thought to tame the problem to the point where action becomes possible.[15] This is especially true in the link between observation and orientation. By the time the loop moves from decision to action, most of the uncertainty should have been resolved, and speed becomes the imperative – here, algorithmic approaches should work well.

Therefore, bounding uncertainty and appropriately throttling AI/ML capabilities accordingly is a key to the ethical and effective use of these technologies. We might even imagine the relationship between expectations under uncertainty and freedom of action granted to algorithms in terms of trust – under conditions of greater certainty, we would be comfortable letting an algorithm accelerate human decision cycles.[16] This is not dissimilar to the 'trust' given to a Sidewinder missile or a sensor in auto-track

mode. Under conditions of lesser certainty, 'trust' would be lower, and we would subject algorithmic findings to higher degrees of human scrutiny and curation. To determine how to bound problem sets for AI/ML systems, we must first understand the relationship between boundaries, uncertainty, and chaos.

Melanie Mitchell's complexity theory

If the Analytical Possibilities Frontier describes how humans and hardware perform under various conditions of complexity, and the OODA loop describes how we create and destroy models to tame complexity, then we can intuit that humans and hardware will have different relationships at each stage of this loop as it proceeds from the complex to the simple. We are missing one piece, however: how do we recognize when a system moves from a complex state to a simple one? In other words, what are the boundary conditions for complexity under different states, and what are the transition points between those states? Consider two hypothetical cases. First, an AI/ML system is tasked with identifying a specific object in a highly congested port. Second, the same system is tasked with identifying that object in the open ocean. Melanie Mitchell's theories of complexity can help to describe the relevant differences between the two cases.[17]

Mitchell's work explores how deterministic or tightly bounded systems transition into chaotic or complex spaces. One classic example of this transition is the 'Reynolds Number' in aerodynamics which describes the transition of airflow over a surface from 'laminar flow,' which is linear and predictable, through a boundary layer, and ultimately to 'turbulent flow,' which is unpredictable and chaotic.

These three regions in aerodynamics are analogous to the decision-making space. There is a set of conditions under which we can reasonably predict events; there is another set of conditions under which the predictability of events starts fracturing into stochastic branches; and there is a final set of conditions under which we can bound an area of uncertainty, but cannot make accurate statements about what is happening inside that bounded space.

These three states help us understand the relationship between complex systems and algorithmic prediction functions. Human heuristics are useful for navigating complex, chaotic, bounded spaces; algorithms less so. But algorithms are ideal for navigating deterministic or stochastic spaces. Therefore, the relationship between humans and hardware should be defined by the level of complexity of the problem set, which can be linked in turn back to the steps of the OODA loop. Under deterministic conditions, we know where something will be; under stochastic conditions, we know where something might be amongst finite options; and under chaotic conditions, we know where something is not.

The kill chain

Briefly, one additional lens through which to view the complexity spectrum is the US military's doctrinal dynamic targeting 'kill chain' in which friendly forces 'find, fix, and finish' enemy targets.[18] The 'find' phase is complex and uncertain. Friendly forces might not know exactly what they are looking for or where to look. As forces proceed from 'find' to 'finish,' the situation becomes less complex and more certain. Throughout the discussion below, we will refer to actions close to the lethal end of the kill chain or far from the lethal end of the kill chain. What we have in mind is, for example, that a system that delivers a kinetic weapon against a target is close to the lethal end, while a high-altitude surveillance system that provides general trend data to analysts and commanders is further from the lethal end of the kill chain.

Data logistics

To consider AI/ML use cases, we need a theory of data logistics – the data management, storage, and communications structures required to train and apply learning algorithms operationally. We situate these data logistics on the feedback cycles of Boyd's loop, since any sensemaking and especially action will rely upon these capabilities. Ontology structures need to be managed to aggregate the volume of data required to train the AI/ML system and resilient storage and communications are required to manage distributed sensors or deploy capabilities that require reachback. More broadly, an AI/ML strategy must tie into a cloud strategy and a data strategy.[19]

Without this supporting structure, developers will struggle to classify algorithms into a 'tightly bounded,' 'loosely bounded,' or 'unbounded' taxonomy across environments. Developers must test an algorithm's reasoning with maximal variance in operating conditions to ensure an algorithm will work equally well across the highest number of circumstances. Current AI/ML algorithms can be extremely brittle. Most algorithms lack a significant ability to generalize outside of the conditions displayed to them in their training data. Even high performance computer vision algorithms display significant performance issues when applied against objects in unusual environments, uncommon orientations, and when algorithmic heuristics are underdeveloped by the depth of their training.[20] Algorithms could rapidly drift between being capable of 'tightly bounded,' 'loosely bounded,' and 'unbounded' control paradigms unbeknownst to the user as micro-details in the algorithm's environment change. Even pixel-level changes to images can severely retard algorithm performance without alerting human operators. To guard against these fluctuations, an algorithm must remain in a continual state of test and development. Like Tesla's 'shadow mode,' military systems might constantly gather data from their current operations and run it against a test algorithm to identify changes in algorithm performance or

logic in real time.[21] Upon deployment to theater, AI/ML-enabled weapon systems will require an initial, human-led calibration and testing period to screen for environmental turbulence that causes the algorithm to operate in ways that would surprise an operator.

Judicious creation of a data logistics theory will expedite the speed at which algorithms achieve full performance in varied operating environments. We might imagine data logistics in the same way that a WWII army imagined industrial logistics – a disciplined ontology is like interchangeable parts, enabling a supply chain to flow. A unit cut off from cloud storage and flowing data loses algorithmic effectiveness over time. Regardless of form, we place data logistics in the background of this model and view it as a prerequisite to all use cases.

Use cases

In this section, we point to three cases that can be applied at the transitional points between steps on Boyd's OODA loop. First, tightly bounded problems (Decide/Act) are precise and can be entrusted to extend human agency toward lethal outcomes. Second, loosely bounded problems (Orient/Decide) are marginally precise and must be refined by human thought to adjudicate between stochastic possibilities before causally connected to lethal outcomes. Third, unbounded problems (Observe/Orient) are imprecise and therefore algorithms deployed in this context should be subjected to a high degree of human scrutiny to navigate chaos before the AI/ML recommendations are adopted.

Use case 1: tightly bounded problems

A tightly bounded case is one in which a human can precisely identify the bounds of a problem. In these cases, the system yields a high degree of accuracy and predictability and is therefore worthy of a high degree of trust even though the outcomes are morally and tactically weighty. Using the lens of complexity, this use case maps onto stable systems. Using Boyd as a lens, this use case helps users transition from Decide to Act. On the Analytical Possibility Frontier, this case trends toward the left side of the graph where algorithms generally perform better than humans.

This use case is the most familiar. The classic AIM-9 Sidewinder was entrusted to home in on a target once a human bounded the problem to an infrared signature lock. In paradigmatic Sidewinder employments, the pilot visually identifies the other airborne entity as an enemy aircraft. The human pilot is capable of this ontological categorization as a result of her education, training, and heuristics. Then, based on the correlation between the audible tone provided by the missile system with the physical location of the enemy aircraft, the human pilot ensures that the thermal signature the missile has recognized and locked onto is, in fact, representative of the

enemy aircraft. The pilot releases the Sidewinder, which then capitalizes on its speed in this 'math-rich' task. The sidewinder then generates a geometric solution to close with the enemy aircraft. All the while, the missile does not 'know' that the signature represents an enemy target. It merely tracks and ultimately targets the thermal signature it was assigned.

AI/ML expands on these possibilities. Suppose instead of a simple thermal signature, the AI/ML tracks a high-resolution signature defined by inputs across the EM spectrum (e.g. visual, radar emissions, thermal). The human operator then assigns this multi-spectral signature on top of an entity that the human has classified as a threat. When such a weapon reported a signature lock on the human-designated-and-evaluated entity, the human releases the weapon to destroy the target. For instance, the human operator might assign the system the task of targeting any signature that exhibits all of the following characteristics: it is hot in infrared; with a radar cross section of W; it emits radiation in frequency bands X and Y; and operates within geographically constrained region Z.

One might suggest here that the constraints in the hypothetical case are unreasonable. One concern many have expressed over so-called autonomous weapons is that they will not be so constrained. But it is precisely this concern that we expect our model to assuage. The human operators employ the system close to the lethal end of the kill chain only because the set of possible targets has been constrained and, therefore, uncertainty has been reduced. These are the same kinds of constraints human operators use to identify targets. For example, during the Cold War, NATO forces could reasonably have assumed that a MiG flying over the Fulda Gap from East Germany toward West Germany is hostile by virtue of its being a MiG on that flightpath. The same would have been true of a T-72 main battle tank actually driving across the Gap. A successful AI/ML weapons system employed close to the lethal end of the kill chain must be subjected to similar constraints.

Use case 2: loosely bounded problems

A loosely bounded case is one in which a human can generally define the signature for an entity, but because of some degree of environmental ambiguity or enemy agency is unable conclusively to correlate signature with entity. AI/ML would nominate potential correlations to a human for adjudication, and the human-machine team would be able to sift through information more quickly than the human could on his or her own and more confidently than the hardware could on its own.[22]

In these cases, the system yields a moderate degree of accuracy and predictability, and can inform weighty outcomes, but requires humans to adjudicate ambiguous cases. Through the complexity lens, these are boundary layer cases in which the system is still discernably operating between several discrete states but does not settle into one clear outcome. In Boyd's

model, this links Orientation and Decision. On the Analytical Possibility Frontier, this case falls near the threshold between human and hardware performance. In this case, the human operator can tell the machine where to look, but not what to look at.

We might imagine a sensor search algorithm that runs at machine speed but that nominates potential targets for human adjudication. As opposed to the tightly bounded case, where we should expect very nearly perfect accuracy (say 99.9+%, using the U.S. military's 'Danger Close' heuristic of 1/1000 incidence of unintended effects), in this case we can imagine a one-in-two, or even one-in-four level of accuracy. These are hypothetical numbers, but they scope a tactical use case where a human deployed their sensor on a rapid search pattern, and confirmed any targets detected. Operators could adjust algorithm sensitivity to reflect environmental conditions, sensor accuracy, or combat intensity. Poor weather might drive someone to accept a higher number of lower probability detections. Conversely, operations in a population-dense urban area might cause users to tune the algorithm to nominate only targets with high probability scores.

Andrew Ilyachinski describes the possibility of camouflage designed to thwart AI – this technique would hamper these tactics by allowing the AI/ML system to report looser correlations.[23] Even so, it should allow detections faster than a standard human search pattern, with the human back-stopping the accuracy of the system. In the tightly bounded case, the human bounds the system prior to deploying it on a task. In the loosely bounded case, the human is re-bounding the loosely bounded problem through this curation process. One set of tactical decisions with these sorts of algorithms will be the reporting threshold. If it is too low, it becomes essentially a human scan, as humans will be constantly adjudicating a very large number of reports. If it is too high, the system will miss targets or threats, especially if an enemy is using effective camouflage. One way to describe this loosely bounded application is as a target nomination process according to which the AI/ML system will suggest targets and human operators will choose from among them which targets to action.

A techno-social challenge for these sorts of systems is the possibility of human overconfidence in AI/ML systems – generally referred to as 'automation bias.'[24] To use such a system ethically, humans must be aware of their own analytical limitations and incorporate context and wisdom into their adjudication rather than merely ratifying a machine solution. In loosely bounded applications, humans will require classroom and experiential training to understand algorithmic flaws and to gain confidence in their ability to diagnose them. Lack of user comfort with algorithmic logic could introduce delays that undercut the technological advantage offered by AI/ML empowered decision-making. Overconfidence in algorithmic logic will introduce a permissive environment in which human operators fail to curate nominated targets. But this phenomenon is not unique to AI/ML systems. If human warfighters overestimate the threat or undervalue

the moral costs of false positives, they, too, will introduce a permissive environment in which they fail to curate potential targets. Adequate training is the solution in both cases.

Use case 3: unbounded systems

An unbounded system is one in which the human cannot constrain a system to the point at which AI/ML can identify entities or act with any appropriate degree of certainty. This case is primarily about anomaly detection – the AI/ML identifies a correlation which challenges a known model or conclusion, or identifies a correlation in an unexpected location without being able to map that correlation onto a characterized behavior, pattern, or entity. Because the AI/ML system is working on pattern recognition, while humans generally think in terms of narrative and causal chains, the AI/ML system might recognize seemingly inexplicable changes in patterns of behavior that humans might overlook. While the resulting reports would often be endogenous or spurious, in some cases they would be accurate and valuable. In these cases, such a tool helps humans turn a critical eye toward their own cognitive frames and biases.

In the language of complexity, these unmoored correlations exist in chaotic spaces, which is why linear causality (and therefore characterization of intent) cannot map onto them cleanly. For this reason, an unbounded system should not be directly connected to lethal force, but should instead serve as an adjunct to human reasoning. Using Boyd's language, this case accelerates and refines the relationship between Observation and Orientation. The case exists on the right side of the Analytical Possibilities Frontier. For a hypothetical expectation of accuracy, one out of a hundred or a thousand nominated correlations might be the needle in the haystack, and such a tool would support brainstorming or increase the rigor of an established model. These are the cases in which the operator doesn't even know where to look yet and the AI/ML system can help the transition from observing the world to orienting toward a particular task or problem set.

We would envision such a use case most relevant to an intelligence analyst looking for an outside-the-box solution the enemy hadn't considered – an analytical 'goat path' around well-set defenses. A program might run Hobbes' regression, 'the correlation of all against all', and find something surprising. Most correlations would likely be endogenous junk, an artifact of chance or circumstance that cannot be changed. But the few that are not junk would be gold.

AI/ML algorithms offer humans opportunities to conduct pattern recognition at scale in unbounded environments. In such scenarios, processing speed and data availability largely replace analyst man-hours as constraints. Geospatial intelligence analysts might use image classification algorithms to search government and commercial satellite coverage of an entire country for weeks, months, or years in search of never-before-seen

military equipment. In a more bounded scenario, human analysts might set rules for an algorithm to notify them each time a piece of equipment outside of the algorithm's ontology appears in an area of importance, e.g. a military base, training area, conflict zone. Alternatively, analysts might ask an algorithm to report on the identification of a specific object class in satellite imagery collected across the planet. Human rights organizations might leverage these same techniques to track refugee flows and locations in a failed state. An NGO could run an algorithm that tracks geolocations of unique dialects or idioms through social media to observe unexpected population movements.

In 1962, human analysts performed the function of anomaly recognition by identifying the Soviet installation of long-range missiles in Cuba, leading eventually to the Cuban Missile Crisis. In the future, AI/ML algorithms will automate this task. Human analysts and scientists will use their area specific knowledge to set rules and bounds and to make requests of algorithms running analysis of nearly unbounded data environments. Human analysts will review algorithmic outputs, focus collection, and explore causal narratives in response to algorithmic observations.

Once again, there is not a direct tactical use case for these sorts of systems. Algorithms running in unbounded environments will consistently nominate 'anomalies,' easily explained away by human general intelligence, context, and cultural knowledge – a zebra in New York City appears like an anomaly until the system incorporates the concept of a zoo. These algorithms are too inaccurate to be responsibly employed at the tactical level because users intentionally place them outside of their logical depth. Analysis of these correlations is time-intensive and inappropriate on a dynamic battlefield. These systems are for the analysis cell or the lab.

If we envision AI/ML through the Heideggerian lens of a prosthetic, these technologies should enable us to extend human agency in three important ways. First, physically, by applying an extension of human agency in places where it would otherwise be impossible such as on a missile in terminal guidance; second, temporally, enabling humans to 'freeze-dry' decisions to enable machines to enact those decisions at extreme speed such as an AEGIS system countering a high-volume, simultaneous time-on-target attack; or third, analytically, by sifting through a time-prohibitive volume of data or an n-dimensional problem, or by removing algorithmic drudgery from human workflows. Since these three forms of prosthetic 'extenders' each have a different relationship to a human ability to 'call-back' the action, they should also map onto our use cases – tightly bounded systems to physical extension of human will such as on a missile beyond datalink range; loosely bounded systems to temporal extension, to be used when time is of the essence but with a human still present; and unbounded systems to analytical extension, improving human insights by accelerating data analytics and challenging heuristics.[25] However, this is an imperfect map. AI/ML can serve as an analytical extender in tightly bounded cases by allowing humans

to divest mindless process and one could argue that temporal and analytical extensions are two instances of the same phenomenon.

Hazard cases

This model suggests at least two ways in which operators might fail to employ AI/ML wisely. In the first kind of error, algorithmic recklessness, users allow an unbounded or loosely bounded system to operate with a high degree of tactical trust to employ lethal force on a battlefield. This evokes the cinematic fears of slap-dash algorithms using lethal force against signatures or behaviors incorrectly classified as hostile. Such a system would likely result in unintended escalation of force or unintended casualties. A desire for the decisive use of force could result in this sort of recklessness, running an algorithm in a complex environment without imposing the requisite constraints.

The opposite hazard case is one in which humans allow an algorithm to provide answers early in the kill chain at an inappropriate level of precision for the conditions and the context. We call this algorithmic abdication. In the Observe and Orient phases of the OODA loop, foreclosing the analytical space too early may accelerate humans toward a clean – but wrong – decision because it is bureaucratically simpler (Figure 6.2).[26]

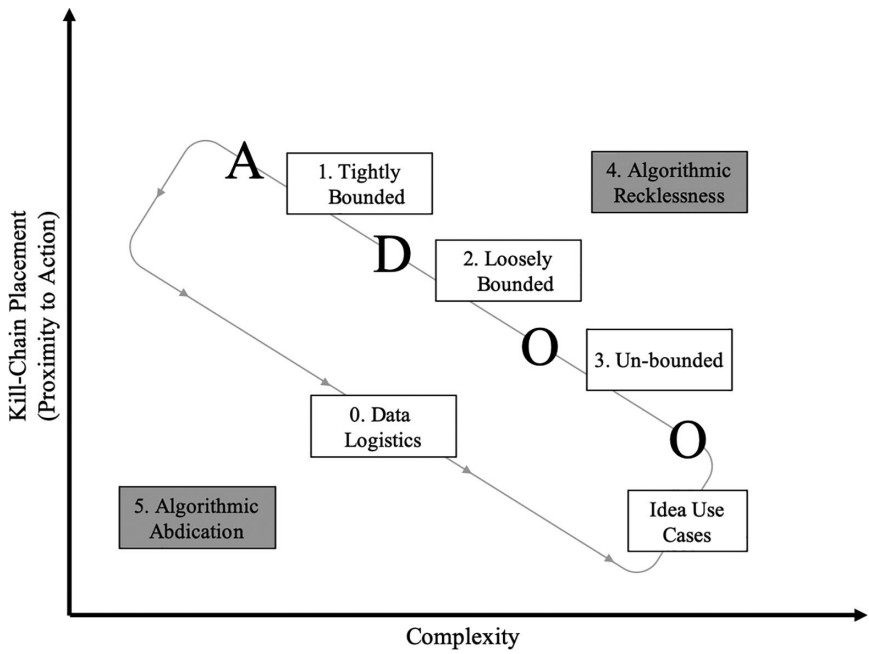

Figure 6.2 Kill Chain Placement-Complexity Graph

Application

Applying this model to the real world generates two important sets of conclusions: one ethical and the other operational. Ethically, the human-centric model for which we argue here disarms some of the ethical concerns that have pervaded the literature. The human-centric model also provides an operational concept to address some of the challenges laid out in the NDS.

Application to ethics

The academic debate over the ethics of AI/ML weapons – often called 'autonomous weapons' – is robust and we lack the space to review it all here. In his summary of the field, John Sullins identifies four categories of concerns: responsibility, rights, virtue, and harm. Here we show how our model helps to mitigate concerns about responsibility and rights.[27]

The responsibility concern was put forward, perhaps most influentially, by Rob Sparrow in 2007. He argued that if weapons systems are capable of selecting their own targets, and those systems err and kill the wrong people, no one – neither the manufacturer, the commander, nor the system itself – is responsible in a meaningful sense.[28] In Sparrow's example, an AI/ML system targets a column of enemy soldiers who are attempting to surrender. The AI/ML recognized the surrender and yet 'had reasons for' targeting them. Sparrow suggests that if a human had committed the same action, he would be tried for a war crime. Though there is the same horrific outcome in this case, there is no one who can be held responsible. If one adopts a machine-centric view of AI/ML systems, then Sparrow might be right. The human was 'out of the loop,' and therefore the AI/ML system was free to commit an action that, in this case, caused wrongful harm.

In our view, however, the human operator is responsible – based on her classroom and experiential training and certification – for matching the machine's degree of freedom with context-specific uncertainty. In Sparrow's case, the AI/ML system is in the 'Decide/Act' phase of the OODA loop (and might, in fact, be navigating multiple OODA steps without human intervention). It is close to the lethal end of the kill chain and is in the stochastic region of Mitchell's complexity spectrum. In our model, the degree of freedom in which the system is operating is not aligned with its position according to the three lenses. A system that is close to the lethal end of the kill chain should be tasked only with tightly bounded problem sets. If the system were bounded in space and time, for example, as in the Sidewinder case, the human operator would be in a position to intervene and accept the soldiers' surrender.

This is just one example and is not meant to show that the human-machine team will not err. The fog and friction of war will play as significant a role in AI/ML applications as it has in all previous applications. What we suggest

here is only that properly bounding the problem with which the AI is tasked ameliorates the responsibility concern.

Sullins' second category of concern is rights violations. Some have argued that to kill someone by 'autonomous weapon' is to disrespect him, and therefore to violate his human dignity.[29] U.S. Air Force General Paul Selva, then Vice Chairman of the U.S. Joint Chiefs of Staff, has said that he does not think it is 'reasonable to put robots in charge of whether we take a human life' because 'we take our values to war'.[30] If the only conception available is one according to which the human might be 'out of' the relevant control loop, then Selva's concern is well-founded. There are two ways in which the conceptual approach we offer here should assuage this family of concerns. First, we can look at the continuity from systems that have been in use for decades and what we propose. Second, we can look again to the constraints under which the AI/ML system is placed when close to the lethal end of the kill chain.

Previously, we discussed an AIM-9 Sidewinder engagement in which the friendly aircraft engages the enemy aircraft at close, visual range. Now consider a different case that has been applied in the real world since at least since 1991.[31] An airborne early warning radar system identifies airborne radar tracks proceeding from enemy territory toward friendly territory. The air battle manager passes those radar tracks to a flight of friendly fighter aircraft that then acquire those tracks with their own aircraft radars. The fighter aircraft employ algorithms to identify the type of aircraft represented by the tracks, and based on that type aircraft identify the tracks as hostile – matching signature to ontology.[32] The flight lead then assigns various enemy aircraft tracks to flight members, and while still some 20 miles away and well beyond visual range, the friendly aircraft employ AIM-120 Advanced Medium Range Air-to-Air Missiles (AMRAAMs) against the enemy aircraft. The AIM-120s conduct the intercept using their own internal radar systems, so the friendly aircraft can conduct evasive maneuvers, remaining outside the enemy's weapons engagement zone.

This case does not involve future technology, but rather existing technology. It is a case of a tightly bounded problem set in which the rudimentary AI system – in this case, the collection of radars, Non-Co-operative Target Recognition (NCTR), and the AMRAAMs – is employed close to the lethal end of the kill chain. Though the pilots chose to release the weapons, the pilots' decisions were informed entirely by human-developed technological inputs – the radar tracks from enemy territory, the formation of those tracks as depicted on his own radar screen, and the target recognition via NCTR – all from beyond visual range. In an engagement like this one, do the friendly pilots violate the enemy pilot's sense of dignity? We suspect that even critics will agree that they do not, because in this case, the pilots chose to kill the enemy combatants.

In our human-centric view, the difference between the case as described and a case of an AI/ML system conducting all the phases of that particular

kill chain is a difference in degree and not in kind. In our view, the human dignity concern is largely diffused, precisely because the closer the AI/ML system is to the lethal end of the kill chain, the more tightly the human operator will bound the problem set. The human operator will have decided in advance that if the radar track represents this type of aircraft with this bearing, range, and course, the AI/ML system should target it. The human is still, in Selva's words, 'in charge of whether we take a human life.'

In general, the conception we propose here mitigates many of the ethical concerns over 'autonomous weapons' precisely because we do not understand them to be strictly autonomous. Instead, we treat them as tools in the hands of skilled human operators who must decide how to bound the problem sets to which they are applied – the human operator must decide how autonomous they should be in a given context. The human operator ensures that autonomy tracks reductions in risk. The higher the risk – of error or loss of life – the less autonomy will be granted to the system.

Application to operations

Embracing our call to reverse the algorithmic warfare paradigm away from Weiner's 'in-the-loop' or 'on-the-loop' to a human-centric decision cycle is essential, not just to inform the academic discussion, but to inform future combat operations.

The 2018 NDS fundamentally changed how the Pentagon envisions conducting future operations. Traditionally, the United States (and generally speaking, 'western' states) implemented a five-phase operational planning construct, which was built around an assumption that the military would have weeks, if not months, to respond to a crisis or crises circumscribed 'over there,' hundreds if not thousands of miles from the continental United States. This has changed with the 2018 NDS. The NDS's four-layered Global Operating Model recognizes that competition with states such as China and Russia is persistent, especially below the level of traditional (Western) armed conflict. The Global Operating Model also appreciates that modern surveillance systems' capabilities, including those enabled by AI/ML technologies in which China and Russia are already heavily invested, make traditional thinking on mass formation maneuver warfare part of a bygone era. This is because it would both take too long to organize the massed formation(s) for employment and the formation(s) would be targeted throughout the entire process. In addition, the Global Operating Model acknowledges that the U.S. military currently has more than 500 overseas bases and tens of thousands of already forward-deployed forces to employ to help implement the NDS.

Hence, the Global Operating Model's first layer is the contact layer, in which forces are to 'expose malign behavior and counter competitor influence' to help provide decision space for policymakers. The second layer, referred to as the blunt layer, includes combat credible and warfighting-oriented forces present forward to deter, degrade, or deny adversary objectives in conflict.

This includes forces specifically designed to deny potential adversary fait accompli strategies in locations such as Taiwan and the Baltics.[33]

The NDS requires elements of the U.S. military to be persistently postured in key maritime regions outside the Indo-Pacific as well such as the regions in and around the Baltic Sea, Strait of Hormuz, and Bab-el-Mandeb Strait. In other words, the NDS requires the U.S. military to become much more distributable, positioned in and around the world's contested maritime littoral regions, with capabilities that can sufficiently deter and, if necessary, deny an adversary attack from achieving its objectives.

In the near future, this construct should be applied to platoon- to company-sized formations of Marines, Soldiers, and special operations personnel from all U.S. military services, equipped with and enabled by AI/ML systems such as loitering munitions. These units should also be distributed persistently in five or six locations in and around the Strait of Malacca, as just one example. These forces should operate alongside U.S. treaty ally military units, as well as with strategic partners – with the main goal of maintaining, if not enhancing the defense of the rules-based order. On a day-to-day basis, these forces would use the aforementioned AI/ML-enabled systems to help identify and counter adversary malign behavior. Predicative logistics-focused algorithms would help ensure the distributed forces do not reach their culminating points. AI/ML-enabled command and control systems would help ensure the forces could communicate, as required, in the parts of the electromagnetic spectrum least likely to be impeded by an adversary. And specific to AI/ML-enabled lethal weapons systems, contact layer forces, as well as those prepared to support them from the blunt layer, would be equipped with loitering munitions – surface, sub-surface, and aerial – that can conduct operations within the bounds imposed by the human operator, despite denied regions of the electromagnetic spectrum. AI/ML would form the technological backbone of a command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) and fires complex capable of dominating key terrain across the Indo-Pacific.

The AI/ML-enabled lethal weapons systems would be designed with defensive purposes in mind, in tightly and loosely bounded scenarios, specifically targeting adversary capabilities required to employ overt military force to overturn the rules-based order. Altogether, these capabilities would enable U.S. forces in the contact and blunt layers to address threats in the expansive Indo-Pacific, at a feasible cost. These forces would also go a long way toward reassuring allies and partners who are currently experiencing, for example, significant coercion and outright bullying efforts by the People's Liberation Army.

Conclusion

This chapter introduced a typology of AI/ML tactical applications by relating the boundedness of a tactical problem to the responsible assignment of lethal

force to that system in the context of the 2018 U.S. National Defense Strategy. Tightly bounded problems allow AI/ML-enabled systems to serve as lethal human proxies, by matching a signature to an entity to a behavior. The human interprets that behavior and those correlations either on the spot, or prior through a database. Loosely bounded systems still have some map between signatures, entities, and behaviors, but deal with more complex environments by referring cases to humans for adjudication. Unbounded systems serve as brainstorming tools by searching for correlations with low context or conceptual maps imposed on those correlations a priori. Humans would then have to determine and test a causal logic, because this technique is inherently endogenous.

This is merely a typology that gives us categories to focus the discussion as we move forward. The harder work of applying these principles will likely need to wait for more direct tactical applications – the technical possibilities will drive more questions as we discover them. But perhaps this model can help us to structure those conversations usefully.

The most important finding in all of these use cases is the relationship between humans and hardware in the context of the contemporary and forecasted future security environment. As always, we should divest 'station-keeping' tasks to the hardware to allow the humans to focus on the 'judgment-laden' tasks. Let the robots do the math, and let the people do the thinking. By properly managing this relationship within each of these use cases, we can take advantage of useful emergence and unexpected events. We have hitherto misunderstood the fundamental problem in AI/ML as 'where does the human sit in or on the control loop'? We should rather determine where AI/ML should aid the human decision cycle.

Ultimately, this approach enables a 'Chaos Imperative' approach to warfighting, allowing a warfighting culture that focuses on reducing constraints on human possibilities rather than increasing constraints in human control (such as in a liberal democracy vice an authoritarian regime) to operate efficiently at higher levels of environmental complexity than its opponent. An anthropocentric view of AI/ML, rather than a cybernetic view of control systems, makes collaboration, initiative, and risk-taking extremely valuable and advantageous commodities.

While this broad strategic employment concept might sound fairly simple, significant obstacles must be overcome to make it a reality. Perhaps foremost among these obstacles, beyond cultural resistance within the military services, is restructuring the AI/ML debate in the academic literature. What is at stake are not machine decision loops devoid of human inputs, but rather human decision cycles aided by AI/ML systems. Next, the military services will need to overcome the lack of current doctrine, training and certification standards, and crucially training ranges to master force employment integration of these AI/ML-enabled capabilities. Without new doctrine, training and certification standards, and places to conduct the required training, it is all but impossible to determine and then evaluate the human decision-making OODA loops required to maximize employment of these capabilities. Many

hurdles remain to integration of AI/ML-enabled capabilities into the U.S. military. How long it will take to complete the majority of this work remains to be seen, but progress can only be made once human and machine interactions are framed appropriately, beyond a pop-culture-driven fear of 'killer robots.' We are optimistic though, especially if the scholarly community embraces the proposed paradigm shift described in this chapter.

Notes

1 The views expressed are those of the authors and do not necessarily reflect those of the U.S. government, the Department of Defense or any of the various service departments.
2 Antoine de Saint-Exupéry, *Wind, Sand and Stars*, Lewis Galantière, trans. (New York: Harcourt Brace & Company, 2010), 46.
3 See, e.g., Human Rights Watch and Harvard International Human Rights Clinic, 'Losing Humanity: The Case against Killer Robots' (New York, 2012), 2, Robert Sparrow and George Lucas, 'When Robots Rule the Waves?', *Naval War College Review* 69:4 (2016), 51, Michael B. Donley and Norton A. Schwartz, 'United States Air Force Unmanned Aircraft Systems Flight Plan: 2009–2047', US Air Force, ed. (Washington, DC: Headquarters, United States Air Force, 2009), 14, 41, Markus Wagner, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems', *Vanderbilt Journal of Transnational Law 47* (2014), 1419, Anton Petrenko, 'Between Berserksgang and the Autonomous Weapons Systems', *Public Affairs Quarterly* 26:2 (2012), 82.
4 James N. Mattis, 'Summary of the National Defense Strategy', ed. Department of Defense (Washington, 2018).
5 Scott Cuomo et al., 'Not yet Openly at War, but Still Mostly at Peace: Exploit the Opportunity to Become the 21st Century Force That Our Nation Needs', *Marine Corps Gazette* (2019).
6 Mike Gallagher, 'State of (Deterrence by) Denial', *The Washington Quarterly* 42:2 (2019): 31–45.
7 Mattis, 'Summary of the National Defense Strategy', 2.
8 In a 2003 study, NASA also used Boyd's OODA loop to assess human-machine teaming. Our approach differs significantly from theirs. See Ryan W. Proud, Jeremy J. Hart, and Richard B. Mrozinski, 'Methods for Determining the Level of Autonomy to Design into a Human Spaceflight Vehicle: A Function Specific Approach' (NASA, 2003).
9 See, e.g., Rebecca Crootof, 'A Meaningful Floor for Meaningful Human Control', *Temple International and Comparative Law Journal* 30 (2016), Michael C. Horowitz and Paul Scharre, 'Meaningful Human Control in Weapons Systems', (2015), Filippo Santoni de Sio and Jeroen Van den Hoven, 'Meaningful Human Control over Autonomous Systems: A Philosophical Account', *Frontiers in Robotics and AI* 5 (2018).
10 Annie Sneed, 'Computer Beats Go Champion for the First Time', *Scientific American (online),* 27 Jan 2016. https://www.scientificamerican.com/article/computer-beats-go-champion-for-first-time/.
11 The Analytical Possibilities Frontier is derived from the economic concept of the 'Production Possibility Frontier,' a depiction of the tradeoffs between making one type of good and another. That model assesses trade between relatively capital-rich and labor-rich countries. See Paul Samuelson, 'Summary on Factor-Price Equalization', *International Economic Review* 8 (1967).

12 Daniel Pink and Clay Shirkey, 'Cognitive Surplus: The Great Spare-Time Revolution', *Wired*, 24 May 2010.
13 Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Abingdon: Routledge, 2007), Ian T. Brown, *A New Conception of War: John Boyd, the Us Marines, and Maneuver Warfare* (Quantico, VA: Marine Corps University Press, 2018), 116–120.
14 John Boyd, *Destruction and Creation* (Leavenworth, WA: US Army Comand and General Staff College, 1987).
15 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).
16 By 'trust' we mean only that a user has a reasonable degree of confidence that the machine's actual behavior will correlate with its expected behavior.
17 Melanie Mitchell, *Complexity: A Guided Tour* (Oxford: Oxford University Press, 2009).
18 See, e.g., Joint Chiefs of Staff, 'Joint Publication 3–26: Counterterrorism', Department of Defense, ed. (Washington, DC: The Joint Staff, 2013), V-3.
19 "Defense Innovation Board", 'Recommendation 12: Forge New Approach to Data Collection, Sharing, and Analysis', Depart of Defense, ed. (Washington, DC, 2016).
20 Amir Rosenfeld, Richard Zemel, and John K. Tsotsos, 'The Elephant in the Room', *arXiv preprint arXiv:1808.03305* (2018). Anh Nguyen, Jason Yosinski, and Jeff Clune, 'Deep Neural Networks Are Easily Fooled: High Confidence Predictions for Unrecognizable Images' (paper presented at the IEEE, 2015).
21 Brad Templeton, 'Tesla's 'Shadow' Testing Offers a Useful Advantage on the Biggest Problem in Robocars', *Forbes*, 29 April 2019.
22 Adam Elkus, 'Man, the Machine, and War', *War on The Rocks* (2015).
23 Ilyachinski, Andrew and Andrew Ilachinski, *Artificial War [Electronic Resource]: Multi-Based Simulation of Combat*, Ebook Central (River Edge, NJ: World Scientific Pub., 2004).
24 Mary L. Cummings, 'Automation and Accountability in Decision Support System Interface Design', (2006), P. Asaro, 'Modeling the Moral User', *IEEE Technology and Society Magazine* 28:11 (2009), Matthew R. Domsalla, 'Rise of the Ethical Machines' (Maxwell Air Force Base: Air University, 2012), Shannon Vallor, '2013 5th International Conference on Cyber Conflict (Cycon 2013)', (2013), Cade E. Bartlett and Nancy J. Cooke, 'Human-Robot Teaming in Urban Search and Rescue' (Los Angeles, CA, 2015), William M. Fleischman, 'Just Say "No!" to Lethal Autonomous Robotic Weapons', *Journal of Information, Communication and Ethics in Society* 13:3/4 (2015), 304, Heather M. Roff and Richard Moyes, 'Meaningful Human Control, Artificial Intelligence and Autonomous Weapons', (Briefing paper for deligates at the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 2016), 3.
25 This concept is similar to Kahneman's system A and B blind spot. See Kahneman, *Thinking, Fast and Slow*, 286–288.
26 See James Q. Wilson, *Bureaucracy : What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989).
27 The arguments that focus on virtue and moral harm have more to do with remotely operated systems than with AI/ML systems and so we set those to one side here. Markus Christen et al., 'An Evaluation Schema for the Ethical Use of Autonomous Robotic Systems in Security Applications', *Digital Society Initiative White Paper Series* (Zurich, 2017), 58–76.
28 Robert Sparrow, 'Killer Robots', *Journal of Applied Philosophy* 24:1 (2007), 66–67. See also Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata', *Ethics and Information Technology* 6:3 (2004), Human Rights Watch, *Mind the Gap: The Lack of Accountability for*

Killer Robots (2015). Tom Simpson and Vincent Müller call the responsibility gap 'the most important argument against killer robots'. Thomas W. Simpson and Vincent C. Müller, 'Just War and Robots' Killings', *The Philosophical Quarterly* 66: 263 (2016), 303.

29 See, e.g., Michael Horowitz, 'The Ethics & Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons', *Daedalus* 145:4 (2016), 31–33; Aaron M. Johnson and Sidney Axinn, 'The Morality of Autonomous Robots', *Journal of Military Ethics* 12:2 (2013), Christof Heyns, 'Human Rights and the Use of Autonomous Weapons Systems (Aws) During Domestic Law Enforcement', *Human Rights Quarterly* 38 (2016).

30 Colin Clark, 'VCJCS Selva Says Us Must Not Let Robots Decide Who Dies; Supports LRSO', *Breaking Defense*, 18 July 2017. For similar concerns, see Noel E. Sharkey, 'The Evitability of Autonomous Robot Warfare', *International Review of the Red Cross* 94:886 (2013), Sparrow, 'Killer Robots', Watch and Clinic, 'Losing Humanity: The Case against Killer Robots'.

31 US Air Force, 'Aim-120 AMRAAM'.

32 See, e.g., John Stillion, 'Trends in Air-to-Air Combat: Implications for Future Air Superiority', Center for Strategic and Budgetary Assessments (2015), 25–29.

33 If contact and blunt layers fail, the final escalatory layer is 'surge,' which will likely entail protracted and costly military conflict. The fourth layer is 'homeland defense' and is relevant independent of the other three layers.

References

Asaro, P., 'Modeling the Moral User'. *IEEE Technology and Society Magazine* 28:1 (2009), 20–24.

Bartlett, Cade E., and Cooke, Nancy J. 'Human-Robot Teaming in Urban Search and Rescue', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 59:1 (2015), 250–254.

Boyd, John, *Destruction and Creation* (Leavenworth, WA: US Army Comand and General Staff College, 1987).

Brown, Ian T., *A New Conception of War: John Boyd, the Us Marines, and Maneuver Warfare.* (Quantico, VA: Marine Corps University Press, 2018).

Christen, Markus, Burri, Thomas, Chapa, Joseph, Salvi, Raphael, Santoni de Sio, Filippo and Sullins, John, 'An Evaluation Schema for the Ethical Use of Autonomous Robotic Systems in Security Applications', University of Zurich Digital Society Initiative White Paper Series, no. 1, 1 November 2017, https://ssrn.com/abstract=3063617 or http://dx.doi.org/10.2139/ssrn.3063617

Christen, Markus, and Burri, Thomas and Chapa, Joseph and Salvi, Raphael and Santoni de Sio, Filippo, and Sullins, John, *An Evaluation Schema for the Ethical Use of Autonomous Robotic Systems in Security Applications* (November 1, 2017). Available at SSRN: https://ssrn.com/abstract=3063617.

Clark, Colin, 'VCJCS Selva Says Us Must Not Let Robots Decide Who Dies; Supports LRSO', *Breaking Defense*, 18 July 2017.

Crootof, Rebecca, 'A Meaningful Floor for Meaningful Human Control', *Temple International and Comparative Law Journal* 30 (2016), 53.

Cummings, Mary L., 'Automation and Accountability in Decision Support System Interface Design', *Journal of Technology Studies*, 32:1 (2006), 23–31, https://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/pdf/cummings.pdf

Cuomo, Scott, Garard, Olivia, Cummings, Jeffrey, and Spataro, Noah, 'Not Yet Openly at War, but Still Mostly at Peace: Exploit the Opportunity to Become

the 21st Century Force That Our Nation Needs', *Marine Corps Gazette* February (2019), 6–22, https://mca-marines.org/wp-content/uploads/2019/02/Cuomo.pdf

Defense Innovation Board, *Recommendation 12: Forge New Approach to Data Collection, Sharing, and Analysis* (Washington, 2016).

Domsalla, Matthew R., *Rise of the Ethical Machines* (Maxwell Air Force Base, 2012). https://apps.dtic.mil/dtic/tr/fulltext/u2/1019463.pdf.

Donley, Michael B., and Schwartz, Norton A., *United States Air Force Unmanned Aircraft Systems Flight Plan: 2009–2047* (Washington, DC: Headquarters, United States Air Force, 2009).

Elkus, Adam, 'Man, the Machine, and War', *War on The Rocks* (11 Nov 2015).

Fleischman, William M. 'Just Say "No!" to Lethal Autonomous Robotic Weapons', *Journal of Information, Communication and Ethics in Society* 13:3/4 (2015), 299–313.

Gallagher, Mike, 'State of (Deterrence by) Denial'. *The Washington Quarterly* 42:2 (2019), 31–45.

Heyns, Christof, 'Human Rights and the Use of Autonomous Weapons Systems (Aws) During Domestic Law Enforcement'. *Human Rights Quarterly* 38 (2016), 350.

Horowitz, Michael, 'The Ethics & Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons', *Daedalus* 145:4 (2016), 25–36.

Horowitz, Michael C., and Scharre, Paul, 'Meaningful Human Control in Weapons Systems', CNAS Working Paper, 2015, 1–16, https://www.files.ethz.ch/isn/189786/Ethical_Autonomy_Working_Paper_031315.pdf

Human Rights Watch, *Mind the Gap: The Lack of Accountability for Killer Robots* (2015), https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots.

Human Rights Watch, and Harvard International Human Rights Clinic, *Losing Humanity: The Case against Killer Robots* (New York, 2012), https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots.

Ilachinski, Andrew, *Artificial War [Electronic Resource]: Multi-Based Simulation of Combat*. Ebook Central. (River Edge, NJ: World Scientific Pub., 2004).

Johnson, Aaron M., and Axinn, Sidney, 'The Morality of Autonomous Robots', *Journal of Military Ethics* 12:2 (2013/07/01 2013), 129–141.

Joint Chiefs of Staff, *Joint Publication 3–26: Counterterrorism* (Washington, DC: The Joint Staff, 2013).

Kahneman, Daniel, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

Matthias, Andreas, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata', *Ethics and Information Technology* 6:3 (2004), 175–183.

Mattis, James N., *Summary of the National Defense Strategy* (Washington, DC, 2018), 1–11, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Mitchell, Melanie, *Complexity: A Guided Tour* (Oxford: Oxford University Press, 2009).

Nguyen, Anh, Yosinski, Jason, and Clune, Jeff, 'Deep Neural Networks Are Easily Fooled: High Confidence Predictions for Unrecognizable Images', Paper presented at the IEEE, 2015.

Osinga, Frans P.B., *Science, Strategy and War: The Strategic Theory of John Boyd* (Abingdon: Routledge, 2007).

Petrenko, Anton, 'Between Berserksgang and the Autonomous Weapons Systems', *Public Affairs Quarterly* 26:2 (2012), 81–102.

Pink, Daniel, and Shirkey, Clay, 'Cognitive Surplus: The Great Spare-Time Revolution', *Wired*, 24 May 2010.

Proud, Ryan W., Hart, Jeremy J., and Mrozinski, Richard B., *Methods for Determining the Level of Autonomy to Design into a Human Spaceflight Vehicle: A Function Specific Approach* (Lyndon B. Johnson Space Center, 2003), https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100017272.pdf.

Roff, Heather M., and Moyes, Richard, *Meaningful Human Control, Artificial Intelligence and Autonomous Weapons*, 2016, http://www.article36.org/wp-content/uploads/2016/04/MHC-AI-and-AWS-FINAL.pdf.

Rosenfeld, Amir, Zemel, Richard, and Tsotsos, John K., 'The Elephant in the Room', *arXiv preprint arXiv:1808.03305* (2018).

Saint-Exupéry, Antoine de, *Wind, Sand and Stars.* Translated by Lewis Galantière, trans. (New York: Harcourt Brace & Company, 2010).

Samuelson, Paul, 'Summary on Factor-Price Equalization', *International Economic Review* 8 (1967), 286.

Santoni de Sio, Filippo, and Van den Hoven, Jeroen, 'Meaningful Human Control over Autonomous Systems: A Philosophical Account', *Frontiers in Robotics and AI* 5 (2018), 15.

Schmidtt, K. P., and Wölfe, E., 'Non-Cooperative Target Identification by Radar: State of the Art and Future', Paper presented at the NATO Research and Technology Organization Meeting, Québec, 22–24 April 1998.

Sharkey, Noel E., 'The Evitability of Autonomous Robot Warfare', *International Review of the Red Cross* 94:886 (2013), 787–799.

Simpson, Thomas W., and Müller, Vincent C., 'Just War and Robots' Killings', *The Philosophical Quarterly* 66:263 (April 2016): 302–322.

Sparrow, Robert, 'Killer Robots', *Journal of Applied Philosophy* 24:1 (2007): 62–77.

Sparrow, Robert, and Lucas, George, 'When Robots Rule the Waves?', *Naval War College Review* 69:4 (2016). 49–78.

Stillion, John, 'Trends in Air-to-Air Combat: Implications for Future Air Superiority', Center For Strategic and Budgetary Assessments, 2015, https://csbaonline.org/uploads/documents/Air-to-Air-Report-.pdf.

Templeton, Brad, 'Tesla's 'Shadow' Testing Offers a Useful Advantage on the Biggest Problem in Robocars', *Forbes*, 29 April 2019.

US Air Force, 'Aim-120 AMRAAM', https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104576/aim-120-amraam/.

Vallor, Shannon, '2013 5th International Conference on Cyber Conflict (Tallinn: Cycon 2013)', 1–15, http://toc.proceedings.com/18867webtoc.pdf.

Wagner, Markus, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems', *Vanderbilt Journal of Transnational Law* 47 (2014), 1371.

Wilson, James Q., *Bureaucracy : What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989).

7 Cyber countermeasures for democracies at war

Nori Katagiri

Cyber activity is one of the most dynamic forms of warfare and poses a tremendous analytical challenge because 'cyber *war*', if it exists at all, is continuous and never conclusive. Moreover, the technology that drives it grows much faster than humans fathom its implications. It is no surprise that the literature of cybersecurity exposes a void in our understanding. One significant lacuna is the question of how nations, especially democracies, wage cyberwar through countermeasures. This is a critical question because, arguably, democratic nations, with high levels of economic prosperity and social openness, are on the defensive. Defending against and deterring cyber attacks is notoriously hard, giving credence to the widespread perception that superiority lies in the offence in cyberwar. In this context, countermeasures offer democracies a useful means of active defence – defined here as the act of counterattacking directly as a means of discouraging future attacks.

This chapter examines the following three areas. First, it investigates how cyberwar has manifested itself in armed conflict over the past decade. Cyberwar has introduced a new dimension to our understanding of warfare and made our strategic environment more complex. As a new domain somewhere between kinetic and non-kinetic dimensions, cyberwar has made it hard for us to put *cyber*security in the traditional analytical framework of *armed* conflict. I seek to clarify the problem by investigating the use of countermeasures as a viable strategy of democracies in defending their cyberspace.

Second, this chapter offers an assessment of how cybersecurity has shaped the character of war at the tactical and strategic levels. I show that democracies' use of countermeasures has complicated the tactical and strategic-level decision-making processes of democracies as they try to secure themselves. The complication stems in large part from a number of constraints that cyber countermeasures impose on democracies.

Third, I draw implications of this analysis for changes and continuities of armed conflict. On the one hand, the arrival of cyberwar has reduced the physical aspect of traditional conflict. New information technology and associated means and methods of delivery have reshaped the conduct of

war. On the other hand, I contend that cyberwar has not changed the fundamentally political character of war. While constraints on democratic countries' use of cyber countermeasures are multi-dimensional – legal, ethical, technical, and strategic – ultimately they can be reduced to a political problem of governance and defence. Both incentives and effects of cyberspace actions remain heavily dependent on the Clausewitzian nature of war as an extension of politics by digital means.

For the purpose of efficiency, I offer minimalist definitions of two key terms – democracy and countermeasures. I use the word democracy in the normative sense to mean a form of liberal democracy with a functional, politically accountable government, rule of law, and free and fair elections, as seen mostly in Western Europe, North America, and parts of East Asia like Japan. I define a countermeasure as a symmetric response to attackers immediately following a verified attack. Countermeasures are an example of active defence strategy, which must be differentiated from passive defence – actions aimed to minimize damage without retaliation. There is an absence of clarity concerning countermeasures in international law, unlike terms which deal with the use of force and armed conflict. This makes it hard to appreciate the utility of international law in this context. It is another reason why it is so difficult for us to analyse cyberwar using the traditional kinetic framework of war. This challenge, however, reflects the political nature of problems among states on the terms of reference. States tend to operate tacitly without definitions.

In the rest of the chapter, the three areas are explored, tackling the question of how democracies fight cyberwar through countermeasures, while highlighting the challenges involved in the process. I suggest that, while countermeasures remain among the most useful means of defending against attacks, democracies continue to struggle to use them effectively. I make this point in three steps. First, I discuss how countermeasures work for democracies. Second, I explore legal, ethical, technical, and strategic challenges they face in using countermeasures. Finally, I draw implications of this analysis for change and continuities of contemporary armed conflict.

How cyber countermeasures work for democracy

Cyberwar has opened a new frontier in the study of warfare and added complexity to the traditional framework of armed conflict. Part of this complexity is the question of whether cyberwar is 'armed' conflict or not. It is a tough question, as states and scholars continue to disagree over what cyberwar means precisely. The disagreement comes in part from the lack of definition of terms like 'use of force' and 'armed attack' in international law. States have agreed to leave them undefined, which means that defining them in cyber contexts is not only hard but impractical. Legal specialists have struggled to define the terms. For instance, the International Group of Experts (IGE), a group specializing in international law applied to

cyber operations, spent a few months deliberating the definitional problems before deciding to let states determine the meaning of the terms their way.[1] Definitions prove difficult because cyber is not considered an independent sphere of conflict but part of a wider context. That is, strategic analysts tend to see cyberwar as a supplement, rather than an alternative, to the traditional armed conflict. The complimentary aspect of cyberwar is a correct approach to adopt, but it also increases the analytical complexity that security scholars must confront.

The introduction of cyberweapons into international security has created various risks for democracies. Socially tolerant and politically open, they present a number of easy targets for exploitation. One of the major challenges they face is the tension between civil liberty and national security, a delicate balance that underscores many recent policy debates and academic discourse.[2] The tension sometimes forces democratic governments to voluntarily restrict the use of force to avoid infringement on pubic rights and escalation with rivals. Among major advanced democracies we witness civil society groups and NGOs promote social awareness on divisive issues like surveillance, censorship, encryption, and privacy invasion. They demand governments act on them and adhere to civil rights. Along with the mainstream mass media, these groups have pressed governments to crack down on digital firms (like Facebook) that are accused of abusing the availability of private information to maximize profit by marketing insecure devices people use to connect through social networks.[3] Former Estonian President Tomas Ilves said that 'Liberal democracies with a free press and free and fair elections are at an asymmetric disadvantage because they can be interfered with – the tools of their democratic and free speech can be used against them'.[4]

One of the best recommendations for democratic countries to defend their cyberspace is made by analysts at places like The Hague Centre for Strategic Studies (HCSS). Among other things, they find democracies' civil society and vigilant government operating within dense networks to be a key bulwark against hostile foreign attempts to undermine social cohesion. In this context, they recommend that democracies confront attackers originating in nondemocratic regimes by respecting the rule of law and protecting the liberal order from foreign meddling. They also call on democracies to develop a variety of measures to deal with disinformation campaigns, including defensive, offensive, preventive, reactive, and proactive measures.[5] One of such measures that democracies have at their disposal is cyber countermeasures. Indeed, democracies may use them primarily by way of active defence retaliation to destroy and degrade enemy capabilities to fight cyberwar. Primary examples of active defence measures are 'hack back' actions that retaliate, 'honeypots' of trapping enemy malware for forensic analysis, and 'dye-packs', a malware in decoy files that traces attackers.[6] These tactics can help introduce false information into adversary networks and generate powerful strategic defences for democracies.

There is no international law that explicitly permits anyone to conduct cyber countermeasures, but there is an emerging norm in favour of them, with some conditions attached.[7] There is a hint that states are entitled to make an in-kind response to cyber attacks as long as they give a warning because the 'attacker' may have been 'spoofed' and used as a conduit by a third party. The IGE, for example, contends that, according to the Tallinn Manuals, governments should be allowed to retaliate on behalf of non-state actors if the attack they have sustained is *attributed* to a foreign state. However, the proposal comes with a caveat that favours nation-states over non-state actors. The IGE claims that it would not 'allow' non-state actors to retaliate for themselves or the governments they may be working with. So it is only states that are 'authorized' to carry out countermeasures. The authorization they have, however, becomes a burden on some states because it can make them more likely than non-state actors to be targeted, and, because non-state actors are not allowed to take their own initiatives to retaliate against attackers, states are the ones that face the burden of protecting *both* themselves and non-state actors they work with (i.e. technology firms that collaborate in government operations). The proposal also gives a somewhat risky impression that concerned non-state actors should only worry about defending themselves when their government collaborators are at greater risk. Further, the way the norms of cyber countermeasures are laid out is complicated. For example, IGE contends that governments should not retaliate against national security proxies that have launched cyber attacks at them (i.e. advanced persistent threat groups) when the attack is not attributed to a foreign state.[8] This proposal, too, essentially protects the proxies even if they are the ones that conducted malicious acts. Inadvertently this therefore gives attackers perverse incentives to make more attacks.

These proposals have not been accepted as fully-fledged norms of cyberspace behaviour. Democracies cannot present these arguments to the international community to justify their own measures when these norms are contested. In fact, even some legal scholars are sceptical towards the Tallinn Manuals. Analysis of state reactions to the Manuals shows many were largely unconvinced when they were published. Dan Efrony and Yuval Shany concluded that

> there appears to be limited support in state practice for certain key Rules of the Tallinn Manuals, and that it is difficult to ascertain whether states accept the Tallinn Rules and wish them to become authoritative articulations of international law governing cyber operations.

As such, they go on to question 'the degree to which the Tallinn Rules are universally regarded as an acceptable basis for articulating the norms of international law governing cyber operations'.[9] The proposals that norm entrepreneurs make to justify state countermeasures have been violated already, as seen, for instance, in Russia's alleged attacks on Ukraine and

Estonia and the US retaliation on Russia's Internet Research Agency for its role in the 2016 US elections. Frustratingly, the international community at large will need time before it decides whether it makes sense to accept these proposals.

The challenges of countermeasures

There are many challenges for conducting countermeasures. The most important point is the political nature of problems associated with cyber countermeasures, specifically that the act of countermeasures may generate a set of tactical and strategic challenges, which, in turn, become political problems for democracies. Cyberweapons are being developed and used as a means of achieving the ultimate ends of national security, and these represent a direct threat to the functioning of democracy. This section will show that many of the challenges they face – be they legal, ethical, technical, and strategic – are associated one way or another with the way democracies govern themselves. Like other forms of war, the core of cyberwar remains political in nature.

Legal and ethical challenges

In many countries, cyber countermeasures are tolerated as a matter of policy and often justified from the standpoint of self-defence, but they can face legal challenges. Even if existing international law makes no ban on cyber countermeasures, some democracies would find it hard to adopt international standards in their domestic contexts and launch them at will. Some democracies may deem it illegal and politically too costly to do even basic (but necessary) things like probing operations into target networks because they prompt lawsuits against governments and commercial operatives and jeopardize the reputation of their leadership. If these countermeasures are revealed and subsequently considered illegal, lawmakers will be held accountable. They would be compelled to clarify their stance, face electoral punishment, or be forced to reveal their modus operandi in cyber defence and thus damage national security. All these concerns make it difficult for them to support countermeasures wholeheartedly. In other words, politicians and cyber warriors face the challenge of executing active defence within domestic legal frameworks.

At the same time, democracies are subject to various principles of international law such as distinction, due diligence, and proportionality (see also Chapters 13–16). Under the principle of distinction, states are obligated to choose targets based on differences between combatants and noncombatants and avoid targeting objects like hospitals, transportation, and a whole range of objects that matter to the survival of the innocent.[10] Only military objects can be targeted in traditional conflict settings, and such an object

is generally considered visible. Of course, it is extremely difficult to distinguish them in cyberspace such as civilian workers who attack democracies on their government's behalf or private sector employees who do the same. Second, the principle of due diligence posits that states should ensure that their territory is not used as a base for cyber operations that affect other states. It is a critical issue in cyberspace because many attacks transit through multiple platforms that are supposed to be politically neutral. Such attacks raise states' obligations to prevent the illegal use of their facilities. Of course, these principles themselves are contested among scholars who disagree over whether neutral states should be held accountable, but most democracies seek to comply with the accepted principles.[11] Finally, the principle of proportionality posits that active defence retaliation, permissible under customary international law, warrants one that is proportional to the first strike. In cyberspace, the problem is that no law or norm clarifies how to measure proportionality. Lack of clarity over measurement raises the chance that countermeasures would be perceived in different manner than that which the democracies intended. The difference in perception of proportionality, which Farrell and Glaser call the 'salience gap', increases the probability of misunderstanding between the attacker and retaliator.[12] Misunderstanding over the measurement of proportionality could lead to unintended escalation.

The major ethical challenge democracies are subject to is to settle with the fact that countermeasures often involve what would be seen as some kind of attack function, even when they are used for defensive purposes. A potential portrayal of the democracy as 'attacker' may contradict with existing international efforts to use cyberspace peacefully. Countermeasures may also provoke the target to counter-retaliate, aiming at the democracy's weakest link – the population. This could put innocent people in direct danger and make them fear that they may become the target of future cyber attacks. Consequently, they may demand government scale down the intensity of countermeasures and comply with the principles of international law. This is a critical matter for democracies, because these groups could, in turn, form a critical mass of norm entrepreneurs with increasingly assertive mass media and NGOs. In addition, democratically elected leaders will face checks and balances from other branches of government and close scrutiny from civil groups. There would be sufficient grounds for people to blame a government for an apparently escalatory policy that did not align with existing efforts to use cyberspace peacefully. Put together, these legal and ethical challenges present democracies a set of constraints that are distinct to their regime type. In contrast, undemocratic states like Russia, China, and North Korea would face less of a challenge in this regard. But the challenges democracies face are even more complex than this single theme. Technical and strategic issues represent problems that are considerably deeper.

Technical challenges

There are three technical challenges. The first is the danger of attacking the innocent by mistake. Just as attribution is hard in cyberspace, locating the right target to retaliate against is just as difficult. This is related to the fact that countermeasures are launched through multiple machines. Technically, this means that countermeasures have the chance of both harming the (innocent) machines outside one's immediate cyberspace and making them part of the operations, raising the question of due diligence. Accurate targeting poses a tremendous challenge for democracies. It requires detailed intelligence as well as scanning and testing of the methods to be used. However, because cyberspace is one of the most guarded national security secrets of any state, getting detailed intelligence requires a high level of training and resources. Further, testing target systems before launching countermeasures is risky because, if detected, it would alert the adversary to the vulnerability and raise the chance of enemy preemption.

Second, use of multiple machines in the process of countermeasures makes it hard for the target to understand the democratic state's intent. To solve the problem may require the democracy to waive its anonymity, but to do so will not be in its interest because it would reveal its capabilities and allow the target to reverse-engineer the malware it received, pass it to others, and actually use it to attack again. An inability to communicate intent fuels the tension between opponents and feeds into what Ben Buchanan calls the cybersecurity dilemma.[13] Because cyberspace is anarchic and intent is hard to read, both sides of a conflict see each other to be aggressive. The dilemma grows because there is nothing that stops them from increasing their capabilities, since it is hard to tell countermeasures from purely defensive operations, and because many believe that offense has an advantage over defence in cyberspace. Anarchy in cyberspace forces democracies to mull attacks but potentially puts them in escalatory cycles that leave them worse off.

Third, countermeasures pose particular difficulties against closed societies.[14] Some targets are hard to reach because they are, according to Henry Farrell and Charles Glaser, 'disconnected from the enemy's external networks or able to function only on dedicated land networks. Other targets may only be accessible through radio frequency operations'.[15] Imagine a cyber operation into North Korea's networks. North Korea keeps external network connections off its citizens but operates an intranet system of a few 'webpages' only elites have access to. Carrying out countermeasures on such systems is hard, because intelligence collection of targets is inaccessible. Only a limited number of specialists could conduct HUMINT, while OSINT is virtually impossible. The technical challenges may sometimes force democracies to 'rely on errors in operational security practices … insiders that have been compromised, or clandestinely conducted physical operations to create or exploit access points unprotected by the authorities'.[16] Democratic states will also continue to face challenges in working with private sector

companies that operate in a politically hostile environment. This is because network contractors that would lay cyber infrastructure across societies would hesitate to do so due to the unreliability of network systems and due to the oppressive nature of these regimes. Conversely, it is also possible that people in democratic countries may feel uncomfortable with allowing foreign tech companies associated with undemocratic regimes like China (e.g. Huawei) to build extensive networks there because they fear that sensitive information may be stolen while also undermining their wider national security.[17]

Strategic challenges

There are three challenges with the strategic use of cyber countermeasures. First, countermeasures require democracies to do a few things prior to launching them, such as drawing a 'red line' and warning attackers not to cross it, and clarifying consequences for attackers. If the line is crossed, they must carry out the threats or lose credibility of future actions. This requires democracies to make a firm commitment. It also requires them to invest heavily in cyber defence even before they launch countermeasures. The commitment requires abundant technical human resources, which may deepen the already severe shortage of skilled labour. The US federal government, for instance, has for years not had enough qualified officials to oversee contracts with cybersecurity firms effectively. Shortage of skilled labour weakens oversight and increases the chance of risks like contractor fraud, waste, and abuse.[18] In other words, countermeasures require heavy investment into both offensive and defensive cyber capabilities *prior to* launching them. Yet in democracies, it may be hard to persuade taxpayers to support heavy investment into offence and defence until the country is actually affected severely by hostile cyberactivity.

The second challenge is that of political expediency. Democracies may sometimes be forced to deploy countermeasures even when the intelligence about a target's culpability, vulnerability, and identity as an attacker is imperfect (as it is most times). After all, countermeasures must be launched in a timely manner for democracy to signal against and discourage future attacks. Yet to do so increases the chance of error, and the cost of such an error can be enormous if the target decides to react in highly aggressive manner. If the democracy hacks back at a wrongly identified actor, it would incur international opprobrium. The mistake would also make the real attacker more emboldened to exploit the lack of assured attribution and retaliation. Aware that democratic nations face the dilemma, attackers would keep attacking.

Finally, countermeasures would generate a problem if they were launched through network contractors whose interests do not neatly cohere with governments. Contrary to public statements otherwise, states have an inherent interest in keeping some distance from network contractors so as to claim plausible deniability whenever necessary. If the distance is too 'close', states

are more likely to be exposed when they get caught. For example, the Italian cybersecurity firm Hacking Team has over the years proliferated surveillance and decryption tools, communication monitoring devices, and systems that can remotely and secretly activate cameras. In 2015, hackers breached Hacking Team to reveal that it did business with governments in Sudan, Kazakhstan, and Bahrain, a corporate secret.[19] Close ties between government and firms were obviously the cause of the revelation. On the other hand, if states operate too 'far' from firms, that causes different types of problems. That is, firms become more likely to act independently of states. Some firms may feel so independent that they disobey orders and falsely claim credit for actions. Behavioural issues force government to monitor them, but the firms may refuse government monitoring to protect corporate and client interests.[20] This dilemma indicates that states have little control over business decisions these firms make or knowledge about for whom the firms ultimately work.

Conclusion

In concluding the chapter, I revisit the book's broader theme by drawing implications of this analysis for change and continuities of armed conflict. On the one hand, cybersecurity has posed an analytical problem for scholars to consider cyberwar in the traditional framework of analysis. Cyberwar can be considered kinetic if it generates casualties through physical damage, but it also has nonmaterial dynamics that only occur within and between computer networks. Yet changes are not confined to analysis and scholarship. Cybersecurity has also made more complex the tactical and strategic calculations of democratic leaders. It has multiplied the number of actors involved and contributed to the complication of decision-making process. Accordingly, decision makers in democracies have to confront a larger number of constraints on the conduct of cyberspace. Because IT continues to evolve, this analysis also sets the stage for future research on related topics. Means and methods of cyber countermeasures have increased the obligation of the international community to assess the nature and impact of IT development and generate a set of legal norms to regulate the malicious use of cyber resources. There is no doubt that we will see AI and other deep-learning machines play a greater role in cyberspace operations.

On the other hand, addition of cyber dimensions to warfare has not changed the fundamentally political character of war. There are so many constraints on the use of cyber countermeasures. Democracies must pay close attention to abide by international law and norms when launching countermeasures. They must also leverage the technological edge they have to increase the effectiveness of the methods while minimizing negative impact of the technical challenges they face. Finally, democracies must stay attentive to strategic logic of the use of active defence to ensure that their actions make more rational sense in their cyber environment. These

constraints continue to profoundly affect the daily lives of ordinary citizens that democracies have the responsibility of defending against cyber attacks. There remain many questions about the effectiveness of countermeasures chiefly because the effect of cyberspace actions remains heavily dependent on the politics of cybersecurity. The impact of cyberwar on the traditional conceptualization of armed conflict is limited, too, because most cyber attacks do not spill over to other domains, and cross-domain cyber operations are rare. But it is also true that democracies, like other states, seek to use cyber countermeasures as an instrument of statecraft. Countermeasures enable active defence to serve as a strategy of attaining security for liberal regimes with absolute mandate to protect citizenry. In the cyber age, the Clausewitzian war as an extension of politics by other means continues to affect our lives.

Notes

1 Michael Schmitt, 'France's Major Statement on International Law and Cyber: An Assessment', *Just Security* (September 16, 2019).
2 Eric Posner and Adrian Vermeule, *Terror in the Balance: Security, Liberty, and the Courts* (Oxford: Oxford University Press, 2007); Gary Gerstle, *Liberty and Coercion: The Paradox of American Government from the Founding to the Present* (Princeton, NJ: Princeton University Press, 2015); Herbert Lin, 'Developing Responses to Cyber-Enabled Information Warfare and Influence Operations', *Lawfare* (September 6, 2018).
3 Susan Laudau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (Cambridge, MA: MIT Press, 2011).
4 Michael Schmitt, 'Grey Zones in the International Law of Cyberspace', *Yale Journal of International Law* 42:2 (2017), 1–3.
5 Sijbren de Jong, Tim Sweijs, Katarina Kertysova, and Roel Bo, *Inside the Kremlin House of Mirrors: How Liberal Democracies Can Counter Russian Disinformation and Societal Interference* (The Hague: The Hague Centre for Strategic Studies, 2017).
6 Michael Chertoff, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (New York: Grove Press, 2018), 188–191.
7 Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defence Option* (Lanham, MD: Rowman & Littlefield, 2018), 174.
8 Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge: Cambridge University Press, 2017), 111–113, 120.
9 Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice,' *American Journal of International Law* 112:4 (2018), 583–657.
10 Schmitt, *Tallinn Manual 2*.0, 414–533.
11 Oona Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Persue, and Julia Spiegel, 'The Law of Cyber-Attack', *California Law Review* 100:4 (2011), 855.
12 Henry Farrell and Charles Glaser, 'How Effects, Saliences, and Norms Should Influence U.S. Cyberwar Doctrine', in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, W. Lin and A. Zegart, eds. (Washington, DC: Brookings Institution Press, 2019), 58–60.

13 Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (Oxford: Oxford University Press, 2016), 3, 141.
14 Herbert Lin, 'Hacking a Nation's Missile Development Program', in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, W. Lin and A. Zegart, eds. (Washington, DC: Brookings Institution Press, 2019), 166.
15 Henry Farrell and Charles Glaser, 'How Effects, Saliences, and Norms Should Influence U.S. Cyberwar Doctrine', *Bytes, Bombs, and Spies*, W. Lin and A. Zegart, eds. 50.
16 Lin, 'Hacking a Nation's Missile Development Program', 166.
17 I thank Rob Johnson for making this point.
18 Irv Lachow and Taylor Grossman, 'Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations', *Bytes, Bombs, and Spies*, W. Lin and A. Zegart, eds., 389.
19 Optiv Security, *2019 Cyber Threat Intelligence Estimate* (Denver, 2019), 16.
20 Tim Maurer, 'Cyber Proxies and Their Implications for Liberal Democracies', *The Washington Quarterly* 41:2 (2018), 172, Lucas Kello, 'Private Sector Cyber Weapons: An Adequate Response to the Sovereignty Gap?' *Bytes, Bombs, and Spies*, W. Lin and A. Zegart, eds., 367.

References

Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (Oxford: Oxford University Press, 2016).

Chertoff, Michael, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (New York: Grove Press, 2018).

Efrony, Dan, and Shany, Yuval. 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *American Journal of International Law* 112: 4 (2018), 583–657.

Farrell, Henry, and Glaser, Charles. 'How Effects, Saliences, and Norms Should Influence U.S. Cyberwar Doctrine', in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Herbert Lin, and Amy Zegart eds., 45–80 (Washington, DC: Brookings Institution Press, 2019).

Gerstle, Gary, *Liberty and Coercion: The Paradox of American Government from the Founding to the Present* (Princeton, NJ: Princeton University Press, 2015).

Hathaway, Oona, Crootof, Rebecca, Levitz, Philip, Nix, Haley, Nowlan, Aileen, Persue, William, and Spiegel, Julia. 'The Law of Cyber-Attack', *California Law Review* 100:4 (2011), 817–886.

Jasper, Scott, *Strategic Cyber Deterrence: The Active Cyber Defence Option* (Lanham, MD: Rowman & Littlefield, 2018).

Jong, Sijbren de, Sweijs, Tim, Kertysova, Katarina, and Bo, Roel, *Inside the Kremlin House of Mirrors: How Liberal Democracies Can Counter Russian Disinformation and Societal Interference* (The Hague: The Hague Centre for Strategic Studies, 2017).

Kello, Lucas, 'Private Sector Cyber Weapons: An Adequate Response to the Sovereignty Gap?' in *Bytes, Bombs, and Spies*, Herbert Lin and Amy Zegart, eds., 357–378 (Washington, DC: Brookings Institution Press, 2019).

Lachow, Irv, and Grossman, Taylor, 'Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations', in *Bytes, Bombs, and Spies*, Herbert Lin and Amy Zegart, eds., 379–400 (Washington, DC: Brookings Institution Press, 2019).

Laudau, Susan, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (Cambridge, MA: MIT Press, 2011).

Lin, Herbert, 'Developing Responses to Cyber-Enabled Information Warfare and Influence Operations', *Lawfare* (2018), https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations

Lin, Herbert, 'Hacking a Nation's Missile Development Program', in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Herbert Lin, and Amy Zegart, eds. (Washington, DC: Brookings Institution Press, 2019).

Maurer, Tim, 'Cyber Proxies and Their Implications for Liberal Democracies,' *The Washington Quarterly* 41:2 (2018), 171–188.

Optiv Security, *2019 Cyber Threat Intelligence Estimate* (Denver, 2019).

Posner, Eric, and Vermeule, Adrian, *Terror in the Balance: Security, Liberty, and the Courts* (Oxford: Oxford University Press, 2007).

Schmitt, Michael, 'France's Major Statement on International Law and Cyber: An Assessment,' *Just Security* (16 September 2019), https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.

Schmitt, Michael, 'Grey Zones in the International Law of Cyberspace', *Yale Journal of International Law* 42:2 (2017), 1–21.

Schmitt, Michael, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second Edition (Cambridge: Cambridge University Press, 2017).

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Part IV

War from above

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

8 Air power 2010–2020

From Helmand to Hypersonics

Johnny Stringer

Introduction

An air power author writing in mid-1991, especially one serving in an air force, would be forgiven for reflecting on the recently fought Gulf War and feeling a sense of achievement and perhaps vindication, as that war had demonstrated to allies, adversaries and competitors just what the fruits of the United States' Second Offset Strategy could achieve. The key constituent parts – satellite navigation, air- and space-based reconnaissance, extensive and secure communications, miniaturisation, precision weaponry and stealth technology, underpinned by exponential increases in computing power – had been employed by the coalition air component with astonishing effect, allowing a 100 hour land campaign with a fraction of the allied casualties that had been predicted. The No Fly Zones that were established throughout the '90s appeared to bear out the idea that the West had pioneered a new way in warfare – a revolution in military affairs even – with air and space power at its core.

The more considered analyst would have seen signs in subsequent air operations over the Balkans and northern and southern Iraq that questioned such confidence. Political and coalition realities and constraints, confused strategic objectives, and the attendant operational challenges had limited or even at times neutered the air instrument. The Kosovo campaign of 1999 might have led some to see it as the zenith of air power; in reality, political pressure and the threat of a land campaign forced Milosevic's hand too.

Ten years' later the score card was more mixed: the Taliban had been removed from power after 9/11, Saddam had been deposed (another showcase for sophisticated joint operations) but in Afghanistan and Iraq the Western coalition was fighting bloody and violent insurgencies, with the land environment the main focus for military and politicians leaders. The seemingly swift and relatively bloodless experience of the 1990s had been replaced by drawn out counter-insurgency (COIN) campaigns, slowly leaching public support and political tolerance. Air power had become an almost wholly tactical instrument, supporting others but not making the decisive strategic campaign contributions of the relatively recent past.

The period 2010–2020 has offered fresh insights into the utility and evolving character of air and space power: continued operations in Afghanistan, whilst simultaneously being employed in to protect the Libyan people from Gadhafi and ultimately allow for his overthrow. Having largely left Iraq by 2011, the West returned in 2014 to fight Daesh, conducting air operations over both Iraq and Syria. This chapter explores air power employment over the last decade in these three campaigns, drawing lessons and deductions from some exceptionally challenging operations in deeply complex environments: geographical, political and informational, but also increasingly shaped by the Information Environment, and with multiple audiences, actors and adversaries. The West and its allies are at an inflexion point in the employment and utility of air and space power, and we no longer own nor can dictate all the terms of the debate.

'The essential glue'

Air and space power are essential to any modern campaign; it would be unthinkable to go to war or to conduct operations without assured access to both domains and thus the possibilities provided by the 'vertical flank'. It doesn't follow that they are employed in the same way regardless of the fight, and thus the actual utility of both has seen different expressions over the last ten years. In Afghanistan, the pre-eminence of the land campaign drove the employment of tactical fast jets, the tasking and collection for Intelligence Surveillance and Reconnaissance (ISR) assets and much of the Air Transport fleet's use too. Both support and attack helicopters provided intimate land support – their raison d'être – to support individual tactical engagements. One could view the Afghan campaign as a series of tactical fights at varying scales, conducted across the country and orchestrated at the regional vice Theatre level. In the United Kingdom, an argument of 'bayonets versus jets' or of tying UK fast jets to UK forces (and thus limiting them to being national and not Coalition/Theatre assets) indicated how polarised understanding and advocacy had become. The debate was only finally concluded when analysis showed that UK ground forces, especially its Special Forces, were getting multiples of Coalition air support in return for each UK air asset provided to the Coalition. This approach also ensured that overall response times across Afghanistan were optimised, as well as allowing tasking of the best Coalition asset to each mission. A similar approach to the initial use of UK helicopter assets also risked effectiveness. Indeed, rotary wing lift had become a strategic and political issue by 2009 as a perceived lack of helicopters forced UK troops to undertake risky moves by vehicle or on foot. Once again, putting the UK rotary wing contribution into a coalition 'pot' and allowing optimum tasking and asset utilisation (provided by an RAF Joint Aviation Group commander) addressed both the tactical challenge and salved political angst. It was also indicative of how in the space of a few years, an understanding of the best use of air power had been allowed to ebb away.

It's not just COIN

Much of our employment of air and space power in the last five years would be familiar to crews operating in Gulf War 1 and through the 90s: of note, the junior aircrew in the first half of that decade are now the senior commanders in their respective air forces. There are generations of operators for whom this way in warfare is a comfortable and well-practised default. Although US-led coalitions had to fight for air superiority and ultimately supremacy at points throughout the period from 1991 to 2003 – the period bookended by the two Gulf Wars – the move to COIN operations for the following ten years had both intended and unintended consequences. For the former, an emphasis on Unmanned Aerial Vehicle (UAV) systems ('drones') to provide extended overwatch and strike was symptomatic of a move away from the primacy of combat air and fast jets. The then Chief of the USAF was fired in 2008, in part for his continued focus on the threats posed by a revanchist Russia and assertive China, and related support for the F22 fighter programme. It could be countenanced by the perceived needs of the current fight and tactical support down to sections of troops, and permitted by our absolute dominance – indeed, ownership – of the electro-magnetic spectrum (EMS). The Taliban could only contest control of the air by largely rudimentary engagements of helicopters, and the occasional success against aircraft at operating locations – the attack at Camp Bastion in September 2012 being the most notable. Coalition access to air- and space-based reconnaissance assets, satellite communications and Precision Navigation and Timing was unfettered.

In Libya in 2011, early strikes to remove the SAM threat in the north of the country allowed the same approach to be employed, although occasional missile launches were defeated by coalition assets. What was fundamentally different was the de facto primacy of the air component: absent a coalition land component, the land campaign was prosecuted by the local Libyan resistance to Gadhafi – effectively as proxy forces – aided by Coalition Special Operations Forces. The paucity of assets and the size of the operating area proved especially challenging: from the 1000+ missions flown in a 24 hour period during Kosovo in 1999, the UK/French-led coalition could launch around 70–80 missions a day in 2011. No wonder that in the immediate aftermath of the campaign, at a closed door debriefing in London, a senior UK Government advisor opined that he was surprised that the Libyan campaign had taken 223 days 'when Kosovo took 78, and it was an easier problem'. Respondents were admirably restrained in their responses.

Air primacy over Libya was exercised through the Combined Air Operations Centre (CAOC) at Poggio Renatico in northern Italy under Lt Gen Ralph Jodice USAF. The strategy for the campaign nominally rested with NATO Joint Forces Command Naples, but the approach devised at Poggio set the terms for how the coalition operated. The air component was back to Theatre-level campaigning and employment, rediscovering

targeting processes (and challenges) almost wholly absent in Afghanistan and needing to explain to the Coalition's political class some of the realities attendant in fighting a state, across the state. Three years later, and coincident with the withdrawal of the bulk of UK forces from Afghanistan and a supposed 'reset' in our campaigning, the danger posed by Daesh (also known as Islamic State in Iraq and Syria – ISIS) forced the West and its allies to begin another Middle Eastern campaign.

Back to Iraq (and on to Syria)

For the United Kingdom, the air operations over Iraq and, subsequently, Syria would generate the most significant and extended air effort since the Second World War. This campaign is also where a number of those factors, apparent over the last 20 years, have been realised, and where the themes noted earlier, and their trajectories, have come together. Indeed, we might be able to identify likely vectors over the next decade. The cautionary note is not to assume that all will emerge or be sustained, and none are likely to be overly dominant or defining. After all, it was only ten years ago that some confidently asserted that COIN was the future of warfare. However, there are contextual, technological, societal, political and multi-domain aspects that are genuinely different and that have likely longevity and impact, especially on the employment of air and space power.

First, the pervasiveness, breadth and penetration of the Information Environment, now amplified by the post-factual, 'fake news' lens through which truth and reality have to emerge, hopefully undistorted. The UK's doctrine and operating concepts are rooted in the importance of securing and maintaining Information Advantage; the default should now be that kinetic actions underscore information operations and not the other way round. For those measuring air power's effectiveness (and national contribution) by counting weapons drops – still a factor in 2017 – this requires fundamental recalibration: input-based measures of activity are no substitute for outcomes-focused Measures of Effectiveness and generate often perverse outcomes. It also speaks to what was known in Afghanistan and became one of the accomplishments of the Libyan campaign, with information-led activity integral to our approach of 'Full Spectrum Targeting'. But it is not yet fully codified, nor should it set activity in only one place on the spectrum: at times, there is still a need to employ precise but significant lethal force to overcome the opponent.

The importance of the Information Environment is matched by that of the Electro-Magnetic Environment and the ability to maintain freedom of manoeuvre across the EMS. Air power is steeped in this (including radar, chaff, jamming and long range communications during the Second World War), but the years in Afghanistan in particular have had a damaging effect on competence and capability. Here, the EMS was ours, and the vital services provided – perhaps most obviously Precision Navigation and Timing and

Satellite Communications, and unchallenged air operations of all forms – were seen as almost a 'free good' at point of use. They were expensive, but they were ours and we built a way in warfare around them. By late 2015, with the first Russian deployments to Syria, this had changed. Although rows of fast jets would have caught the eye, the most significant Russian capabilities were advanced double digit SAMs, communications and GPS jammers, and a sophisticated Radar and C2 network. Without firing a round or rocket, the deployment altered the operational context for coalition air assets, and generated a new, genuinely strategic set of challenges. This Anti-Access Area Denial (A2AD) umbrella in the eastern Mediterranean covered the key UK air base at Akrotiri and threw its protective bubble over Russian land, air and maritime assets. As noted previously, we knew this was coming – it was an inevitable counter to our way in air warfare prosecuted so successfully over 25 years. Noteworthy too that the imagery – iconography perhaps – of Russian military strikes looked remarkably familiar to that first seen in 1991: the overt emphasis on equivalence masked the reality of Russia's employment of 90 per cent unguided weapons and the terror bombing of civilians in Aleppo and other cities.

Contextual and campaigning evolution

Societal and political factors have had increasing bearing on the use of air power and on the conditions governing its employment, and on the technologies within the instrument itself. Drones have been a bellwether for this phenomenon, and the UK experience is instructive. The RAF has operated Predator A and B drones (the latter the more advanced and capable Reaper model) since early 2005, but the United Kingdom elected to stay almost silent on their operations for several years. This de facto vacuum was filled by others, stating or insinuating various nefarious or even illegal activities on which they were employed. Belatedly, the curtain was pulled back a little but the United Kingdom remains on the back foot, even when the reality is that drones are effectively conventional aircraft that happens to have a cockpit and crew several thousands miles distant. Political considerations will always inform operational policy, and the codified expression of this – allied to international law and conventions – are national Rules of Engagement (ROE). Syria and Iraq have presented substantial targeting challenges as noted previously; the years of targeting individuals in unoccupied expanses of desert have not fitted military personnel well for the realities of employing precise but lethal force in dense urban environments against opponents for who the people are targets, shelter, revenue and recruits. As the air component Commander during the operations to liberate Mosul and Raqqah, every day posed numerous targeting challenges; keeping senior staff in the United Kingdom informed on these – and how we were overcoming them within the ROE – was 'vital ground' in maintaining trust and confidence in our judgement and decision making. The proximity of multiple actors

provided further complexity: the battle space in Iraq and especially Syria was and is the most congested, contested, competitive and at times confused that any of us can recall in the last 30 years. The potential for tactical-level errors to have strategic consequences was ever present and required consistently good analysis and judgement, often from relatively junior personnel in the CAOC and from coalition aircrew.

We should also reflect on the realities of campaigning in coalition, viewed from the perspective of the air component. If ROE reflect national policy positions, then it is axiomatic that they will differ across nations although all will be legally compliant: this translates into mission types or target sets that one or more nations might be unwilling or unable to conduct or prosecute, even if they have the professional and technological ability. It is also a truism that the more meaningful the contribution, the greater the level of political and other risks nations must be willing to accept. Once again, tactical limitations can have unforeseen strategic and/or campaign consequences. Commanders must continually review their permissions and delegations to ensure they are appropriate for ever-evolving missions and be willing to argue for refinement if necessary. It may also be that standing ROE have been deliberately limited; the case for unlocking them has to link the tactical requirement and benefit with the oversight that will ensure risks are managed and kept below the agreed threshold. This will almost certainly require high level government and ministerial approval: commanders must possess the advocacy and antennae to operate in this environment too.

Operations against Daesh also provided the best example yet of integrating effects across multiple domains. With air- and space-based assets collecting ever-increasing imagery, signals intelligence and other intelligence data, their centrality to rapid understanding is a given; the ability to fuse this with all source intelligence – including from our cyber operations – is where real and decisive advantage is rooted. Multi-Domain Integration across tactical, operational and strategic levels remains a work in progress and is not yet our default setting, but we have made significant inroads in recent years. The work in late 2016 and early 2017 to understand Daesh's Vehicle Borne Improvised Explosive Device (VBIED) capability and then target it across the enterprise represents an excellent example of both opportunity and challenge. A conventional approach might have sought to 'soak' likely areas of interest with the ISR assets we could muster (but prejudicing other high priority tasks) and have strike assets on call to engage (but tying them geographically and by mission). Instead, patient and imaginative interagency work allowed the coalition to understand how Daesh developed and fielded their VBIED capability – down to what we could call the lines of development – and the CAOC staff then refined its intelligence effort against key nodes. Given the commercially available Chinese drones used by Daesh, alongside those built by their own nascent armaments 'industry', this included activity many miles from the battlefield. The challenge, beyond maintaining necessary operational security, included preserving tactical

and operational patience across coalition HQs, where early strikes would have failed to achieve the overwhelming effect of coordinated action. The simultaneous strikes conducted in early 2017 were a precursor to a number of other similarly well-integrated actions as the physical 'Caliphate' was reduced to its final few square miles.

Regaining our advantage

Much of the above speaks to a 'democratisation' of what previously were high end capabilities, the product of expensive and leading edge technology and thus for many years largely the preserve of top tier Western nations, much of it from the United States. Today, traditional competitors have achieved at least near-peer status in almost all areas of air and space power; worryingly, their investment in countering and exploiting the EMS whilst we were focused on violent but relatively unsophisticated COIN campaigns has been well worth the cost. Western nations are playing catch up, rethinking old lessons on resilience and dispersal whilst regaining competence – if not yet competitive advantage – in areas such as hypersonic weapons. Western air power is challenged at both ends of the spectrum too: Daesh drones may have been unsophisticated when compared to a Reaper, but were employed across four of the five core air power roles – intelligence, strike, command and control, and counter-air (when attacking Russian aircraft at Hmeimim Airbase in Syria). As with the cyber domain, the price of entry is now remarkably low, and imagination in employment has a value all of its own. It is also worth reflecting that digital and IT connectivity allowed Daesh to mass produce weaponry to remarkably precise tolerances at multiple sites – from mortar rounds to the stabilising fins for repurposed 40mm grenades, dropped by drones on Iraqi Security Forces and the forces of the Syrian Democratic Front. Daesh drones represented their own air power capability, whilst the raft of commercially available satellite-supplied or enabled information, data and communications made them space power users. Our own technological advances were being used against us. Equally, this provides vulnerabilities for us to exploit and it is entirely reasonable to see as much upside here as downside. If one pulled the key tenets of the last ten years of air and space operations, including capability development and across allies and adversaries, the following key themes are apparent and can be argued to have genuine longevity – we will need to be active and anticipatory if we are to continue to maintain and regain advantage.

We will operate continually and fight episodically; success in the former, and especially in the 'grey zone' of sub-threshold and hybrid military activity will limit the latter. How we deploy our air assets as 'routine business' will thus need to simultaneously reassure, deter, provide training and force development/experimentation opportunities and be integral to our messaging and our narratives. It is unlikely that their operations will be solely single domain-specific and they will almost certainly need to nest with multiple

military, security and other lines of operation. In the recent past, we have at times struggled to maintain the right relationship between the Diplomatic, Information, Military and Economic (DIME) lines of operation: successful military operations can be for nought if they are significantly out of alignment with, or outpacing, actions in these three other key areas. Increasingly, failure to understand and operate with agility within the Information line might be the difference between success and failure. We will also need to strike the right balance between demonstrating capability (as well as resolve) whilst keeping our most advanced capabilities and tactics secret and secure. This will only accelerate the move towards synthetics and the need for high fidelity synthetic environments within which we will train, test and experiment – routinely across multiple domains too. Our actual environments will be increasingly complex – Iraq and Syria are a foretaste of this. Global population growth and competition for resources will fuel much of this through the myriad malign consequences that will flow. We are likely to see urban operations as increasingly common (they were pivotal in both Libya and against Daesh) as population growth in cities continues across the world.

As a result, the nature of command in the air environment will almost certainly change too. Senior air commanders are too comfortable with the tactical and the technological; those who have gained recent operational command experience have been frustrated by the institutional inertia and memory that privileges joint command to those from other components, notably the land environment. The USAF is investing heavily – conceptually, financially and in its people – in Multi-Domain Operations. This, and key enabling elements such as the Combat Cloud, speaks to a step change in how air and space operations are planned, integrated and conducted in the future. This will need commanders with the experience and insights traditionally prized, married with the ability to exploit digitisation in its many forms and to 'visualise' courses of action and possible outcomes in ways we have not been able to before. The opportunities of 'digital twins' and routine, cross-government and multinational exercising will be a commonplace. We will need to develop our people differently than at present – something the United Kingdom has recognised across its joint Professional Military Education. We will move beyond both the autodidact and professionally curious, whilst the most talented will find his or her career a rich experiential and developmental pathway where air force posts are planned against those in the joint/integrated force and even interagency. Solely being the best tactical operator is not going to cut it, but operational experience and the realities of combat will still have both a premium and a value.

Most importantly, our way in air warfare will need to change, and our developing ways in space and cyber will need to be imaginative and unconventional. Arguably, we should recognise that the 'Third Offset Strategy' already exists and is that developed and employed by our adversaries. We have continually developed and refined second offset technologies and

their employment; in doing so, much our 'playbook' has been studied by others and effective counters developed to limit or neuter our advantage. Some are asymmetric and beyond a 'counter-force' solution: Russian and Chinese information operations are now a commonplace – from elections to pandemics – and financial muscle affords influence across multinational fora. All help create a favourable geo-strategic context within which to exercise multiple levers of national power, including the military. The West 'won' the Cold War through multiple means, including targeted spending on advanced capabilities that the USSR could not afford to match. We do not have that luxury now; indeed, one could argue that both China and Russia are in a 'sweetspot' of technological development, affordability, near/actual peer capability and deployable mass. We will need to think and do differently.

Technologies and tempo

Encouragingly, the main strands of what could represent that new way in air warfare are in either conceptual or actual development. The technologies of the second offset strategy will continue to be developed, because used intelligently they continue to confer relative advantage. If attempting to negate them requires significant and active use of the EMS, then this helps develop our understanding and provides opportunity for both hard and soft counters; some of these means will be from other domains to allow required operations in air and space. As such, the individual domain concepts that we develop will need a unifying purpose at their heart and will – by design – be interoperable and integrated to an extent not seen before. For coalitions and alliances, the trick will be to bring different nations up to the required level routinely, and able to be more sophisticated when required. Sharing information seamlessly across multiple classifications and fusing myriad sources will be essential; harnessing the potential of Artificial Intelligence, Machine Learning and Human Machine Teaming will make sense of the vast data lakes of information, sorting wheat from chaff and allowing human engagement ever further up the value chain. This, in turn, will accelerate and multiply Boyd's OODA loop in a way that its inventor would have approved. Faster, more accurate understanding will allow swifter, better decision making and – allied to a raft of pan-domain effects and those exercised on the Diplomatic, Information and Economic lines – generate multi-domain tempo that we see infrequently at present. Nor is this wishful thinking: all of these aspects were employed against Daesh in 2017 albeit occasionally, and doubtless elsewhere. More worryingly, they have also been employed at least in part against us too. We will need to leverage the variety of talent and free (not 'permitted') thinking across our alliances and partners – a strength of democracies and a weak point for autocracies. And air forces will need to be more focused on the need to engage and shape public and political understanding and debate about emerging technologies.

We are rightly bound by higher legal, moral and ethical standards than our opponents and must continue to be; but without engagement and education, we run the risk of investing multi-billions yet having technologies without permissions. One relevant area is Autonomy and the extent to which human approval within a potentially lethal targeting chain is required or provided: Human On or In the Loop is thus not an arcane intellectual talking point, but a fundamental decision for national polities as they look to develop and employ future technologies within their forces.

A more profound question might be whether air and space become – for air, return to – genuinely strategic domains where our actions offer both strategic choice for us and dilemmas for our opponents. From Overy to O'Brien, historians have noted how, in the Second World War, Western air power underpinned and enabled a strategic war fighting concept that avoided heavy attritional land campaigns – as suffered by the Soviets in the east as they finally overwhelmed an equally attrited Wehrmacht. Thereafter, it was used as a continuous campaigning tool and method, whether in its own right or in concert with land and maritime power. In an early example of integrated activity to secure Information Advantage, we might think of the fusion of air and maritime power with ULTRA intercepts from Bletchley Park to win the Battle of the Atlantic. It is then more than a little disappointing that we have allowed our thinking on the air instrument and its strategic utility to atrophy over the last few decades, content to be a supporting junior component to the supposedly more important activity being done by others. We have lost the sense of air power as a political instrument too, just at the time where the strategic context – and the need when continually 'Operating' to be able to protect, engage and constrain – places a premium on this attribute.

Final reflections

It would be brave and a little foolish to unthinkingly re-energise the claims made by early air power theorists, but where ambition then outpaced technology, it might be true that it is now our ambition that is in lag. Our air and space operations of the last decade have been at the heart of a Western way in warfare, but an over-emphasis on technology and tactics has often stymied assessment of what strategic purposes air power can service – in short, what it is for and what it allows. The emphasis placed on COIN operations saw the dangers of 'Main Effort' becoming sole effort realised, and we are still dealing with the unintended consequences when developing air and space power capabilities that are fitted for an era of persistent competition. However, we have inspiration and example to draw upon over many decades, and from its earliest days air power was seen as a strategic instrument. It continues to offer political choice: the drawn out, Land environment-dominated campaigns in Iraq and Afghanistan generated political risks, whilst both Libya and the campaign against Daesh have

highlighted the agility and flexibility of air power, even if political outcomes have been or remain uncertain. Air power has an inherent and innate capacity for integration too, across domains and with the widest array of agencies and organisations: the standard operating procedures that allow complex multinational air operations are the wellspring for this, and the time/speed/distance-crunching potential of both air and space platforms speak to agility and responsiveness. We might usefully reflect on whether we need to reconnect with what this affords at the operational and strategic level, rather than over-concentrating on the technological and tactical as ends in themselves. Our opponents certainly have.

References

Elliott, Christopher, *High Command, British Military Leadership in the Iraq and Syria Wars* (Oxford: Oxford University Press, 2015).

Gaddis, John Lewis, *The Cold War* (London: Allen Lane, 2005).

Gray, Colin S., *Airpower for Strategic Effect* (Maxwell: Air University Press, 2012).

Lee, Peter, *Reaper Force, the Inside Story of Britain's Drone Wars* (London: John Blake, 2018).

Meilinger, Philip, *Bomber, the Formation and Early Years of Strategic Air Command* (Maxwell: Air University Press, 2012).

Mueller, Karl P., *Precision and Purpose, Airpower in the Libyan Civil War* (Santa Monica, CA: Rand Corporation, 2015).

O'Brien, Phillips Payson, *How the War was Won, Air-Sea Power and Allied Victory in World War II* (Cambridge: Cambridge University Press, 2015).

Olsen, John Andreas, *Airpower Applied, US, NATO and Israeli Combat Experience* (Annapolis: Naval Institute Press, 2017).

Olsen, John Andreas, *Routledge Handbook of Air Power* (Abingdon: Routledge, 2018).

Overy, Richard, *Why the Allies Won* (London: Pimlico, 2006).

Pape, Robert, *Bombing to Win, Air Power and Coercion in War* (New York: Cornell University Press, 1996).

Ricks, Thomas E., *The Gamble, General Petraeus and the Untold Story of the American Surge in Iraq, 2006–2008* (London: Allen Lane, 2009).

Simms, Brendan, *Unfinest Hour, Britain and the Destruction of Bosnia* (London: Penguin, 2001).

Strachan, Hew, *The Direction of War, Contemporary Strategy in Historical Perspective* (New York: Cambridge University Press, 2013).

9 Armed drones, technological momentum, and the character of war

Johannes G. Postma

Introduction

If there is one weapons system that has come to symbolize warfare in the early 21st century, it is the unmanned aircraft or drone.[1] From pocket-sized Black Hornets deployed at the platoon level to RQ-4 Global Hawks with the wingspan of a Boeing 737 used for strategic intelligence, drones have secured their place in military arsenals around the world.

Drone proliferation has skyrocketed. Both states and non-state actors increasingly use drones to achieve their military and political objectives. At the turn of the century only a handful of technologically advanced states possessed the capabilities to deploy drones over the horizon to deliver effects on the battlefield. Twenty years later insurgent groups such as Islamic State (IS) and Hezbollah are known to have used drones to drop explosives on their adversaries.

This chapter sets out to answer two questions: first, how has armed drone technology manifested itself in the conduct of war, and second, do armed drones determine the character of warfare or are they merely a new tool for humankind to use. This last question focuses on who or what has agency in this dynamic: humans or the machine? The first section evaluates the use of armed drones during the last two decades and assesses the effects of this new technology on the conduct of war. Extensive empirical data relevant to this subject are hard to come by because many states shroud their armed drone programs in secrecy. The significant proliferation and increased use of armed drones, however, provide a rich evidentiary base to draw on. Armed drone technology is an evolution of the new Western way of war characterized by risk aversion, precision, and the use of air power. Drones create opportunities for decision makers to execute missions that were impossible or very difficult to execute before. Paradoxically, however, the proliferation of drone technology to an increasing number of actors has increased risk on the battlefield to Western military forces, as operators of armed drones, whether advanced military systems or modified consumer drones, can now take to the air to hold their adversary at risk.

Building on these observations, this chapter uses the academic debate on technology and human agency to provide a perspective on the question if

the rise of the armed drone is akin to opening Pandora's box or if the drone genie can still be kept in the bottle. One of the recurring arguments on the part of drone critics is that the development of armed drones will lead to more autonomous systems and a dehumanization of war. They attribute technology with a level of agency that suggests that the technology itself determines its use. Drone advocates, on the other hand, argue that drones are just another tool in the toolkit, not much different from traditional weapons systems, and that humankind will remain in control of how these are deployed.[2]

This chapter finds middle ground between these determinist and social constructivist schools by using the lens of technological momentum. The theory of technological momentum holds that social factors and human behaviour drive technological development, but that as technological systems grow, they acquire momentum and their external impact becomes more deterministic. The review of drone operations over the last two decades shows these dynamics at play. However, this chapter also demonstrates that, even though drones' momentum may be growing at a significant rate, opportunities remain for human intervention.

Armed drones and the character of war

There is a degree of reciprocity in the relation between armed drone technology and warfare. Drones are as much shaped by the changing character of war as they shape it. A review of armed drones' track record over the last 20 years shows that the technology was developed as part of a new way of warfare that gained traction in the late 20th century. This Revolution in Military Affairs (RMA), which took place around technological advances in information processing, communications, precision weapons, stealth, and the use of space assets, created the environment in which unmanned armed aircraft became possible. As drone technology matured and proliferated it reinforced some developments that were set in motion by the RMA, while arguably spurring new changes as well. Three observations stand out in the analysis of how armed drones changed and were changed by the character of war in the last two decades.

First, armed drones have become the posterchild of a type of warfare that is characterized by the minimization of risk incurred by military practitioners and political decision makers in the deployment of military force. This trend goes back to the 1990s when the first drones were used over the Balkans and air power was the weapon of choice to deliver military effects while minimizing the threat to own forces. As a means of 'virtual war', 'immaculate warfare', or 'risk transfer warfare', drones allowed their operators to project military force over vast distances without putting friendly forces in harm's way.[3] As drones were weaponized after the turn of the century, they came to represent an evolution of this new way of war. The successful traits of air power (precision, speed, and reach) were combined

with the persistence and low risk to friendly personnel that drones could offer. This new way of war, made possible by armed drone technology, has to a degree removed human interaction from the battlefield as it wages war primarily through technological means. Some academics have expanded this argument to claim that classic warfare in which honour was a key trait has been pushed side by post-heroic warfare in which only calculations of risk and effect matter.[4] Other schools of thought point to the growing disconnect between the people who project power and the dynamics on the battlefield itself. Andreas Krieg and Jean-Marc Rickli describe this as surrogate warfare:

> Weaponized UAVs (Unmanned Aerial Vehicles) opened a new chapter of warfare in which drones can increasingly be used as surrogates. They allow the transfer of the burden of war to the machine, enabling the military commander to spare the infantryman from operational risk while allowing the policymaker to achieve military objectives discreetly and with plausible deniability.[5]

The coalition fight against IS in Iraq is an illustration of this surrogate war, as Western states did not deploy massive troop numbers, but instead relied on a combination of human proxies (Iraqi Security Forces and Peshmerga) and technology (armed drones).

The second observation is that armed drone technology has expanded the mission sets that its operators can draw from. Drones' inherent capabilities provide decision makers with opportunities they did not have before. This leads to what Michael Boyle calls goal displacement:

Drones feed

> a process by which an organization enlarges its ambitions and begins to substitute alternative, sometimes more expansive, goals for the ones that it originally had,' or more straightforward, 'drones are cheap, so we can throw them at a problem and see what happens'.[6]

The most telling example of this dynamic is the rise of targeted killings and signature strikes by the United States. As early as 2002, only a year after the MQ-1 became operational in the Afghan theatre, the United States used an MQ-1 in Yemen to target and kill Qaed Salim Sinan al-Harethi, the alleged mastermind behind the bombing of the USS Cole in 2002, in Yemen. This was the first of a long series of targeted killings that spans three US Administrations. Within a decade, drones came to be the 'only game in town in terms of confronting or trying to disrupt the Al Qaeda leadership', CIA Director Leon Panetta said in 2009.[7] Targeted killings take place outside of recognized theatres of war, far from the battlefields of Afghanistan, Iraq, or Syria. The hotspots for these types of attacks are alleged terrorist safe havens in Pakistan, Yemen, and Somalia. These drone strikes target terrorist

leaders who are planning attacks, supporting insurgencies, or engaging in other nefarious activities that pose a threat to the security of troops on the ground in warzones, or to Western societies. Terrorist leaders tend to seek shelter in inaccessible regions or in failed states that, wittingly or unwittingly, offer them protection. Conventional interventions or military action are, therefore, less palatable. Drones offer a solution to this problem; they are the weapon of choice for Washington when it comes to striking these targets without risking friendly lives or jeopardizing US popular support. In the first year of his presidency, President Obama launched more drone strikes than the total number of strikes during both G.W. Bush Administrations.[8] The use of drones under President Trump has not shown any signs of decrease. In total, according to the Bureau of Investigative Journalism, the United States executed 968 targeted killings between 2002 and 2020 in Pakistan, Yemen, and Somalia.[9]

Further goal displacement is noticeable within the covert campaign of targeted killings. In the early 2010s, the Obama Administration issued new targeting guidelines that would stretch the legal boundaries of armed drone use. As the counter-terrorism campaign ramped up, Washington authorized drone attacks on persons whose identity was not known, but whose behaviour or pattern of life suggested terrorist activities. These 'signature strikes', as they came to called, widened the aperture for drone operators to attack targets when nefarious behaviour was suspected. According to some analysts, these signature strikes have stretched the targeting guidelines to a point where it has become impossible to justify these under international or US domestic law.[10] Targeted killings and signature strikes are examples of goal displacement that was the result of the availability of armed drones. These examples show that the availability of drones changed the way wars were fought as they became a 'solution looking for a problem'.[11]

A corollary to this change in warfare is the idea that the threshold for the use of military force has lowered because of the introduction of the armed drone. States, the argument goes, are more likely to start a war as armed drones provide relatively low-risk options to intervene where boots on the ground are unfeasible or politically unacceptable. Walsh and Schulzke argue that 'the possibility of drones contributing to the overall case for military interventions cannot be disregarded'.[12] Michael Boyle concurs:

> Drone technology might have brought the United States the capability of continuously monitoring and striking targets remotely, but it also led the United States to lose sight of its goals and drift into a growing number of conflicts worldwide.[13]

The third observation on the influence of armed drones on the character of war is somewhat paradoxical. Since the end of the Cold War, Western powers have looked at air power as one of the most effective and risk-free tools at their disposal to fight wars far away from home and with minimal risk to

friendly lives. Air power was the weapon of choice in the conflicts in Afghanistan and Iraq as it gave coalition powers a technological advantage that terrorist and insurgent groups were unable to counter. Drone technology constitutes a next evolutionary step in this reliance upon air power. This holds an interesting paradox as the proliferation of drone technology has created opportunities for other actors, both state and non-state, to level the playing field to a certain extent and make use of air power instead of being on the receiving end of it.

Insurgent groups have taken to the skies and use drones in their military operations. Houthi rebels used drones to attack Saudi oil facilities in December 2019.[14] Groups such as Hezbollah, Al Qaeda, Taliban, and IS are also known to have added drones, armed and unarmed, to their arsenals.[15] These drones in the hands of insurgents and terrorists will typically not be as advanced as those operated by state actors; yet, even with limited capabilities, non-state actors can use drones to hold their adversaries' forces and targets at risk. This dynamic played out during the fight against IS in Iraq and Syria. As a US general remarked:

> The most daunting problem was an adaptive enemy who, for a time, enjoyed tactical superiority in the airspace under our conventional air superiority in the form of commercially available drones.[16]

IS would use consumer drones to guide mortar fire or attach small explosives and drop these over Iraqi and Peshmerga forces. According to Pablo Chovil, drawing from his operational experiences in Iraq, these drone operations by IS had a significant effect on the fighting will and morale of Iraqi forces.

Despite its clear military and technological superiority, the coalition to defeat ISIL [Islamic

> State of Iraq and the Levant] in Iraq faltered in the face of devices that a 20-year-old with no formal military experience could easily obtain on Amazon. These cheap and easy-to-use devices, previously little more than toys, herald a democratization of technology on the battlefield that will change the way nations contend with adversaries.[17]

Do drones shape war?

If drone technology does indeed change warfare by providing low-risk means to project military force and thus makes new types of mission such as targeted killings possible, the question becomes whether drone technology has agency of its own as it continues to gain importance in modern warfare. This section aims to provide a nuanced perspective on the question if armed drones do indeed open Pandora's Box, or if the genie can be kept in, or put back into, the bottle.

The debate on the role of technology in human history serves as a lens to formulate an answer to this question. Drone critics tend to have a deterministic perspective on the role of drones in dehumanizing war. Drone advocates, on the other hand, use social constructivist arguments to claim that humans will remain in control of the machine. These opposing schools of thought seem irreconcilable at first glance. The rift in this debate, however, can be bridged by using Thomas Hughes' theory of technological momentum. This theory, which finds a middle ground between technological determinism and the social construction of technology, sufficiently explains the influence of drone technology on the conduct of war, while it points to possibilities for human intervention to reign in the deterministic properties armed drones have acquired over the years.

Technological determinism

Technological determinism considers technology as a driving force behind social change. Technological solutions can solve social problems, and technology itself has agency. This means that the use of technology is determined by the shape and capability of the technology itself, rather than by a conscious social process that utilizes this technology. Robert Heilbroner, a leading technological determinist, captures this in two hypotheses. The first is that there is a 'determinate sequence of productive technologies for those societies that are interested in originating and applying such a technology'. Heilbroner further argues that 'the technology of a society imposes a determinate pattern of social relations on that society'.[18] In short, technology drives history. Following Heilbroner's logic, armed drones are a logical evolution of the development of weapon systems that has gone from horses, to tanks, to aircraft, to drones, just as 'the steam-mill follows the hand-mill not by chance but because it is the next stage in the technical conquest of nature that follows one and only one grand avenue of advance'.[19] Taking this logic to its next iteration, drone critics argue that armed drones will lead to increasingly autonomous systems, which will, in turn, cause dehumanization of warfare with far-stretching moral and ethical implications.[20]

Goal displacement as observed in the targeted killing and signature strike campaigns is a telling example of a deterministic dynamic. To drone critics, there is a clear causal relationship between the availability of drones and the way they are used to execute targeted killings and signature strikes. As Audrey Cronin puts it: 'The problem for Washington today is that its drone program has taken on a life of its own, to the point where tactics are driving strategy rather than the other way around'.[21] Technological determinists would argue that this is a clear example of technological systems determining social change. The availability of drones pushed US Administrations to change the manner in which they target high-value terrorist targets. Drones shaped warfare. Without drones, the argument goes, these leadership strikes would be impossible to execute. Thus, technology shapes

strategy, and allowing drone technology to mature unbounded will create further goal displacement or mission creep in future warfare.

Determinists paint a gloomy picture of future warfare as armed drones continue to develop into more autonomous systems. They envision a Pandora's box that will open and swarms of drones that 'jointly decide their plan of attack, engage the enemy – and beat the hell out of 'em of course – all without direct human intervention'.[22] These ideas of a dehumanization of war are deeply rooted in the determinist approach to armed drones and form a stark contrast with the school of social constructivism.

Social constructivism

Social construction of technology combines concepts from technology studies and sociology and holds that new technologies are developed, selected, or rejected by social forces. Pinch and Bijker, as two of the leading proponents of this school, argue that 'the social environment […] shapes the technical characteristics of the artifact' and that 'the social groups that constitute the social environment play a critical role in defining and solving the problems that arise during the development of an artifact'.[23] Social constructivism, therefore, opposes technological determinism as it posits that social forces create technological change.

Social forces vary in their source. The truncated version of Clausewitz's paradoxical trinity provides a helpful framework to categorize these.[24] Passion, reason, and chance, embodied by people, commander, and government, have all played a role in the rise of armed drones. First of all, as the earlier review has shown, societal pressures to minimize the risk to own forces played a crucial role in the development of unmanned systems. Western societies grew more risk-averse and sought ways to minimize the threat to the military forces they sent to do their bidding, as well as by extension to limit the threat to their society itself. The invention and development of armed drones were initiated and catalysed by these social forces. A similar line of reasoning can be construed for the government leg of the trinity. As Krieg and Rickli argue, political leadership was confronted with a dilemma in these post-modern societies as they still had to deploy military force to far away conflicts while the public appetite for these missions had diminished.[25] Drones provided a solution as they offered a risk-free and clean way to fight a war. Finally, armed drones are an ideal weapons system for military commanders, who are always obliged to weigh the expected tactical or strategic effects of a mission against the associated risk to their forces. Any solution that maximizes the military effect while minimizing the risk to friendly lives will be wholeheartedly supported. In the words of Lt gen (ret) David Deptula: 'The real advantage of unmanned aerial systems is that they allow you to project power without projecting vulnerability'.[26]

Constructivist drone advocates will further argue that armed drones are logical evolutions of manned platforms that increase effectiveness while

minimizing risks. Most of the missions drones perform are identical to what their manned counterparts do. Armed drones are extensively used for traditional missions such as armed overwatch of ground troops or Close Air Support (CAS). Drones are optimized to perform the dull, dirty, and dangerous tasks and do so exceedingly well over modern battlefields due to their persistence, sensor capabilities, and the ability to deliver precision strikes.

Armed drones provide technological answers to the social demands by the people, the government, and military commanders. Core to the social constructivist argument is the concept that technology is shaped by social forces that spark new technologies in order to satisfy social demands to the way wars are fought. Warfare shapes drones. In this reasoning, humans will always be in control of armed drones and the technological system itself has no agency. This puts this school of thought at direct odds with technological determinists.

Technological momentum

The drone debate is characterized by a polarization in which determinist critics and constructivist advocates are divided by irreconcilable differences over who ultimately has agency over the development of armed drones: humans or technology. This has created a stalemate that is unhelpful as we face a future in which drones will undeniably continue to be an important tool on the battlefields and beyond. Therefore, it is important to recast the debate and attempt to find a middle ground which allows for constructive discussions on how armed drone technology can be harnessed, preserving its advantages while mitigating risks.

The theory of technological momentum bridges both schools and provides that middle ground. The theory, by Thomas P. Hughes, posits that all technological change is initiated by societal and cultural input, but that over time as the technology matures, it gains momentum and obtains deterministic properties.[27] Furthermore, Hughes argues that it is possible to change the direction of a technological system even when it has gained considerable momentum. '[W]e must remind ourselves that technological momentum, like physical momentum, is not irresistible'. [28]

Technological momentum grows as systems mature and gain political, economic, and value components. [29] Armed drones score well on all three, and as their momentum increases so will their deterministic properties. Politically, as discussed earlier, armed drones provide a valuable tool to decision makers to project military power while mitigating military and political risks. Drones have become a weapon of choice. Economically, the market for armed drone technology is booming. According to January 2020 statistics gathered by Drone Wars UK, 17 state actors have armed drones in their inventory, and another ten are near to obtaining them. [30] The global military drone market is estimated to grow by at least 30% over the next

decade, expanding by $98 billion.[31] The widespread use of armed drones on the battlefields and their significant proliferation also add to the value component. Drones are slowly but steadily becoming the new normal for states and non-state actors around the world. This effect is compounded by the significant increase of drones outside of the domain of war and warfare. More people are being exposed to the presence of drones in society. Drones are everywhere, from toy quadcopters flown in backyards to industrial-sized drones used for mapping and ground analysis purposes. This widespread presence of drones has normalized the technology as a whole, which adds to the technological momentum of the system.

These observations suggest an increasing momentum for armed drones, and, following Hughes' theory, a concurrent increase in their deterministic properties. The theory of technological momentum, however, reminds us that this momentum is not unstoppable and that we are not on a predetermined glideslope towards robot wars. Human intervention through social forces is possible at all times, even though Hughes does argue that changing a system becomes harder as it grows larger. The evidence of attempts to limit armed drones by social pressure is as visible in the last decades as are the cases that show their increasing deterministic properties. As armed drones gained influence and affected the character of war by goal displacement and making risk-free wars possible, the social forces intervening in this development grew stronger.

Human rights organizations and NGOs are the most vocal voices of these social forces. Much of the discussion on the legality and ethical implications of armed drones takes place within the United Nations. Special Rapporteur Ben Emerson wrote an influential report in 2014, in which he called for 'international consensus on the applicable legal principles'.[32] The United Nations Institute for Disarmament Research runs a research program aimed at promoting structured dialogue among states to increase transparency, oversight, and accountability of armed drones.[33] NGOs also contribute to efforts to limit the rise of armed drones. PAX, a Netherlands based peace organization actively involved in the drone debate, for example, warns for the expanding proliferation of small and cheap armed drones to state and non-state actors around the globe. Their 2018 report recommends establishing global regulations on the use of armed drones and setting up an export control framework.[34]

These are just some examples of social forces at work to change the course of armed drones as a technological system. While these and similar reports and debates have not led to significant new international laws and regulations regarding the use of armed drones, they do indicate an expanding global movement that aims to limit the use and proliferation of armed drones. This movement is a social force that cannot be ignored by global actors as they continue to integrate armed drone technology into their militaries. Therefore, the social forces exerted upon armed drones by various actors affect how states develop and use these weapon systems. Technological momentum can be resisted, and Pandora's box can still be closed.

Conclusion

This succinct analysis of the use of armed drones and the relation between technology and warfare leads to two conclusions. First, armed drones have indeed changed the character of war by creating new opportunities for political leaders as well as military commanders. The possibility to project power over vast distances while minimizing the risk to own forces, as an exponent of the new Western way of war, has led to an increase in the use of armed drones and an expansion of the mission sets these systems are tasked with. This has significantly affected the way military force is brought to bear on, and beyond, the battlefield.

Furthermore, drones have given insurgents and terrorist organizations capabilities to take to the skies and use rudimentary forms of air power to level the playing field against more technologically advanced adversaries. The introduction of armed drones and the wider proliferation of drone technology to disparate actors on the battlefields have thus set in motion a paradoxical dynamic. While drones were developed under social pressures to minimize risk to friendly forces, the exponential proliferation of drone technology has also pushed unprecedented capabilities into the hands of potential adversaries, creating more risk for friendly forces.

Other drawbacks that accompany these changes are also noticeable. Armed drones have been deployed to execute targeted killings and signature strikes, stretching the legal borders of the Laws of Armed Conflict and raising questions of legitimacy. On a more philosophical plane, the rise of armed drones begs the question if this technology has introduced a new post-heroic way of war that is far removed from our paradigmatic images of war involving clear actors with large numbers of troops on distinct battlefields striving for a decisive victory. Are armed drones the harbingers of a new paradigm in warfare, allowing actors to project power by selective violence at continuous low levels of intensity without crossing the Rubicon towards war?

The second conclusion this analysis presents is the reciprocal relation between armed drones and warfare. Armed drones were developed to provide technological solutions to social, political, and military problems. As they matured, however, they gained deterministic properties and started to change the ways wars are fought. Drones, therefore, shape and are shaped by the character of war.

This paraphrase of the theory of technological momentum offers a pragmatic perspective on the correlation between the rise of a new complex technological system and the ever-changing character of warfare. Thus, this perspective finds middle ground in the debate on drones between the critics whose arguments can be nested within the theory of technological determinism on the one hand, and drone advocates who stress the advantages of drones and argue that humankind will maintain agency over their development and use on the other hand. This analysis shows that it is not one or the

other, but rather that a reciprocity exists between the technological and the social forces that meet in the complex human interactions during war and conflict.

Approaching the rise of drones through this lens allows for a more nuanced analysis of the role of drones in the modern conduct of war, which reconciles the differences between drone advocates and critics. The technological system of armed drones is undeniably gathering significant momentum and thus gaining deterministic properties. This momentum is not irresistible, however, and the system is still pervious to social forces that can alter its course. It is not technology itself that determines how it is used in wars, now and in the future. Humankind will always maintain leverage over the technological system to change its use and further development.

Notes

1 Unmanned aircraft go by many names and acronyms such as Unmanned Aerial Vehicle (UAV), Unmanned Aircraft System (UAS), or Remotely Piloted Vehicle (RPV). For consistency, this chapter will use 'drone' as it is the common vernacular that describes the gamut of various unmanned aircraft.
2 For more thorough analyses of this debate see Avery Plaw, Matthew S. Fricker, and Carlos R. Colon, *The Drone Debate: A Primer on the US Use of Unmanned Aircraft Outside Conventional Battlefield* (Lanham, MD: Rowman & Littlefield Publishers, 2016), and Frans Osinga, 'Bounding the Debate on Drones', in *Moral Responsibility & Military Effectiveness*, H. Amersfoort et al., eds. (The Hague: Asser, 2013), 244–278.
3 See, respectively, Michael Ignatieff, *Virtual War: Kosovo and Beyond* (New York: Picador, 2001); Stephen D. Wrage, ed., *Immaculate Warfare: Participants Reflect on the Air Campaigns over Kosovo, Afghanistan, and Iraq* (Westport, CT: Praeger, 2003); Martin Shaw, *The New Western Way of War: Risk-Transfer War and Its Crisis in Iraq* (Cambridge: Polity, 2005).
4 Christian Enemark, *Armed Drones and the Ethics of War: Military Virtue in a Post-Heroic Age* (London: Routledge, 2014).
5 Andreas Krieg and Jean-Marc Rickli, *Surrogate Warfare: The Transformation of War in the Twenty-First Century*, *Transformation of War in the Twenty-First Century* (Washington, DC : Georgetown University Press, 2019).
6 Michael J Boyle, *The Drone Age: How Drone Technology Will Change War and Peace*, Ebook (New York: Oxford University Press, 2020), 74.
7 Noah Shachtman, 'CIA Chief: Drones 'Only Game in Town' for Stopping Al Qaeda', *Wired*, May 19, 2009., https://www.wired.com/2009/05/cia-chief-drones-only-game-in-town-for-stopping-al-qaeda/.
8 Jack Serle and Jessica Purkiss, 'Drone Wars: The Full Data', *The Bureau of Investigative Journalism*, 2017, https://www.thebureauinvestigates.com/stories/2017-01-01/drone-wars-the-full-data.
9 Ibid.
10 For a case study on the legality of signature strikes, see Plaw, Fricker, and Colon, *The Drone Debate*, 147–154.
11 Thomas P. Hughes, 'Technological Momentum', in *Does Technology Drive History?: The Dilemma of Technological Determinism*, M. Roe Smith and L. Marx, eds. (Cambridge, MA: MIT Press, 1994), 110.
12 James Igoe Walsh and Marcus Schulzke, 'The Ethics of Drone Strikes : Does Reducing the Cost of Conflict Encourage War?' (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2015), 37

13 Boyle, 239.
14 Jonathan Marcus and Katie Prescott, 'Saudi Arabia Oil Facilities Ablaze after Drone Strikes', *BBC News*, September 14, 2014, https://www.bbc.com/news/world-middle-east-49699429.
15 Boyle, *The Drone Age*, 436.
16 General Raymond A. Thomas III quoted in Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats*, Combating Terrorism Center at West Point 2018, https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf.
17 Pablo Chovil, 'Air Superiority Under 2000 Feet: Lessons from Waging Drone Warfare against ISIL', *War on the Rocks*, May 14, 2018, https://warontherocks.com/2018/05/air-superiority-under-2000-feet-lessons-from-waging-drone-warfare-against-isil/.
18 Robert Heilbroner, 'Do Machines Make History?', in *Does Technology Drive History?: The Dilemma of Technological Determinism*, Merritt Roe Smith and Leo Marx, eds. (Cambridge, MA: MIT Press, 1994), 56–59.
19 Ibid., 55.
20 See for example Laurie Calhoun, *We Kill Because We Can: From Soldiering to Assassination in the Drone Age* (London: Zed Books, 2015), and Medea Benjamin, *Drone Warfare: Killing by Remote Control* (London: Verso, 2013).
21 Audrey Kurth Cronin, 'Why Drones Fail: When Tactics Drive Strategy', *Foreign Affairs* 92:4 (July/August 2013), 44.
22 Benjamin, *Drone Warfare,* 218.
23 Wiebe E. Bijker, Thomas P. Hughes, Trevor Pinch, eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 2012), 7.
24 Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1984), 89.
25 Krieg and Rickli, *Surrogate Warfare*.
26 Lieutenant General (ret.) David Deptula quoted in Grégoire Chamayou, *A Theory of the Drone*, Janet Lloyd, ed. (New York: The New Press, 2015), 12.
27 Thomas Hughes first introduced the theory of technological momentum in 1969: Thomas Parke Hughes, 'Technological Momentum in History: Hydrogenation in Germany 1898–1933', *Past & Present* 44 (April 6, 1969): 106–132, http://www.jstor.org/stable/649734. An updated version can be found in Thomas Parke Hughes, 'Technlogical Momentum', in *Does Technology Drive History?: The Dilemma of Technological Determinism*, Merritt Roe Smith and Leo Marx, eds. (Cambridge, MA: MIT Press, 1994), 102–113.
28 Hughes, 'Technological Momentum', 113.
29 Ibid., 112.
30 Drone Wars UK, 'Who Has Armed Drones?', https://dronewars.net/who-has-armed-drones/. Accessed on March 29, 2020.
31 Jon Harper, '$98 Billion Expected For Military Drone Market', *National Defense Magazine*, accessed April 16, 2020, https://www.nationaldefensemagazine.org/articles/2020/1/6/98-billion-expected-for-military-drone-market.
32 Ben Emmerson, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Ben Emmerson' (2014), https://undocs.org/A/HRC/25/59.
33 John Borrie, Elena Finckh, and Kerstin Vignard, 'Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles' (2017), https://www.unidir.org/publication/increasing-transparency-oversight-and-accountability-armed-unmanned-aerial-vehicles.
34 Wim Zwijnenburg and Foeke Postma, 'Unmanned Ambitions: Security Implications of Growing Proliferation in Emerging Drone Markets', 2018, https://www.paxforpeace.nl/media/files/pax-report-unmanned-ambitions.pdf.

References

Benjamin, Medea, *Drone Warfare: Killing by Remote Control* (London: Verso, 2013).

Bijker, Wiebe E, Hughes, T.P., and Pinch, T., eds., *The Social Construction of Technological Systems : New Directions in the Sociology and History of Technology* (Cambridge, MA : MIT Press, 2012).

Borrie, John, Elena Finckh, and Kerstin Vignard, 'Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles' (2017), https://www.unidir.org/publication/increasing-transparency-oversight-and-accountability-armed-unmanned-aerial-vehicles.

Boyle, Michael J., *The Drone Age: How Drone Technology Will Change War and Peace* (New York: Oxford University Press, 2020).

Calhoun, Laurie, *We Kill Because We Can : From Soldiering to Assassination in the Drone Age* (London: Zed Books, 2015).

Chamayou, Grégoire, *A Theory of the Drone*, Janet Lloyd, ed. (New York: The New Press, 2015).

Chovil, Pablo, 'Air Superiority Under 2000 Feet: Lessons from Waging Drone Warfare Against ISIL', *War on the Rocks*, May 14, 2018. https://warontherocks.com/2018/05/air-superiority-under-2000-feet-lessons-from-waging-drone-warfare-against-isil/

Clausewitz, Carl von, *On War*, Michael Howard, Peter Paret, and Bernard Brodie eds. (Princeton, NJ: Princeton University Press, 1984).

Cronin, Audrey Kurth, 'Why Drones Fail: when Tactics Drive Strategy'. *Foreign Affairs* 92:4 (July/August 2013), 44–54.

Drone Wars UK, 'Who Has Armed Drones?', April 5, 2019. https://dronewars.net/who-has-armed-drones/

Emmerson, Ben, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Ben Emmerson', 2014, https://undocs.org/A/HRC/25/59.

Enemark, Christian, *Armed Drones and the Ethics of War : Military Virtue in a Post-Heroic Age* (London: Routledge, 2014).

Harper, Jon, '$98 Billion Expected for Military Drone Market', National Defense Magazine, Accessed April 16, 2020, https://www.nationaldefensemagazine.org/articles/2020/1/6/98-billion-expected-for-military-drone-market.

Heilbroner, Robert, 'Do Machines Make History?', in *Does Technology Drive History : The Dilemma of Technological Determinism*, Merritt Roe Smith and Leo Marx, eds., 56–59 (Cambridge, MA: MIT Press, 1994).

Hughes, Thomas Parke, 'Technlogical Momentum', in *Does Technology Drive History?: The Dilemma of Technological Determinism*, Merritt Roe Smith and Leo Marx, eds., 102–113 (Cambridge, MA: MIT Press, 1994).

Hughes, Thomas Parke, 'Technological Momentum in History: Hydrogenation in Germany 1898–1933', *Past & Present* 44 (April 6, 1969), 106–132.

Ignatieff, Michael, *Virtual War: Kosovo and Beyond* (New York: Picador, 2001).

Krieg, Andreas, and Rickli, Jean-Marc, *Surrogate Warfare: The Transformation of War in the Twenty-First Century* (Washington, DC : Georgetown University Press, 2019).

Marcus, Jonathan, and Prescott, Katie, 'Saudi Arabia Oil Facilities Ablaze after Drone Strikes', *BBC News*, 2014. https://www.bbc.com/news/world-middle-east-49699429.

Osinga, Frans, 'Bounding the Debate on Drones', in *Moral Responsibility & Military Effectiveness*, H. Amersfoort, R. Moelker, J. Soeters, and D Verweij, eds., 244–278 (The Hague: Asser, 2013).

Plaw, Avery, Fricker, Matthew S., and Colon, Carlos R., *The Drone Debate: A Primer on the U.S. Use of Unmanned Aircraft Outside Conventional Battlefields* (Lanham, MD: Rowman & Littlefield, 2016).

Rassler, Don, *The Islamic State and Drones: Supply, Scale, and Future Threats*. Combating Terrorism Center at West Point, 2018, https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf.

Serle, Jack, and Purkiss, Jessica, 'Drone Wars: The Full Data', The Bureau of Investigative Journalism, 2017. https://www.thebureauinvestigates.com/stories/2017-01-01/drone-wars-the-full-data.

Shachtman, Noah, 'CIA Chief: Drones 'Only Game in Town' for Stopping Al Qaeda', Wired, n.d. https://www.wired.com/2009/05/cia-chief-drones-only-game-in-town-for-stopping-al-qaeda/.

Shaw, Martin, *The New Western Way of War: Risk-Transfer War and Its Crisis in Iraq* (Cambridge: Polity, 2005).

Smith, Merritt Roe, and Marx, Leo, *Does Technology Drive History?: The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994).

Walsh, James Igoe, and Schulzke, Marcus, 'The Ethics of Drone Strikes: Does Reducing the Cost of Conflict Encourage War?', Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College Press, 2015. http://purl.fdlp.gov/GPO/gpo64804.

Wrage, Stephen D., ed., *Immaculate Warfare: Participants Reflect on the Air Campaigns over Kosovo, Afghanistan, and Iraq* (Westport, CT: Praeger, 2003).

Zwijnenburg, Wim, and Postma, Foeke, 'Unmanned Ambitions: Security Implications of Growing Proliferation in Emerging Drone Markets', 2018, https://www.paxforpeace.nl/media/files/pax-report-unmanned-ambitions.pdf.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Part V

War from the ground up

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

10 The challenge of territory-governing insurgencies on war and peace strategies

Paula Cristina Roque

> When a country is being subverted it is not being outfought; it is being out-administered.
>
> Bernard Fall

Introduction

Many insurgencies hold territory within and across state boundaries today, seeking to define a new nation or society, or to form a new state. Governing territory allows these groups to survive militarily and logistically, through political and social embeddedness. Territory-governing insurgencies, which define the building of parallel states as pivotal to their struggles, are growing in number and pose challenges to national and international policymakers in their efforts to resolve intractable conflicts and build peace. These insurgencies are not new but require a more precise and detailed understanding. In Africa there are Al-Shabaab in Somalia, the Azawad movements in Mali, the Boko Haram factions in Nigeria and the ex-Seleka in the Central African Republic, among others. Elsewhere, the Houthis and Al-Qaeda in the Arabian Peninsula in Yemen, the Taliban in Afghanistan, the Islamic State (IS) in the Levant, and the Kurdish Democratic Union Party (PYD) in Syria, among others, lead sub-national, national or transnational wars aimed at (re)constructing political orders. To provide differentiated responses to these insurgencies, new ways are needed to understand them, so as to develop policies that are fit for purpose.[1] In a post Covid-19 world, where sovereignty, government, citizenship and locality will suffer deep transformations, military groups that govern their constituencies will most likely increase and cement their authority.

These insurgencies differ in many aspects, as each is a product of specific local and regional contexts and has distinct conflict drivers. However, they are not a new phenomenon. In Africa several operated in the post-independence era in Mozambique, Angola, Sudan, Ethiopia and Uganda. Elsewhere, in Sri Lanka, Colombia, Palestine, Lebanon insurgencies performed government functions in their territories. Today, groups that govern territory and civilian populations differ widely. Some movements emerged from prior

wars while others began on their own. Some are secessionist, while others are reformist. Some are transnational and fed by regional rivalries, while others are locally defined yet active regionally. All carve out constituencies in need of liberation to correct the failings of past liberations. Some mobilise around utopian ideas and outcomes that aim to transform existing social, political and territorial orders, weaving in religious, sectarian, subnationalist, anti-imperialist, anti-establishment and revolutionary themes. These insurgencies no longer believe that justice, fairness and power can be harnessed through existing political configurations. They therefore propose to establish new political orders. The impact of such insurgencies and their parallel states on domestic populations disrupts societal cohesion and threatens coexistence between states. When they prove organisationally resilient and ideologically persuasive, with the ability to consolidate constituency support and govern territory effectively, they can render insurgent wars intractable.

Numerous factors favour their continued emergence as well as explain why these insurgencies have survived despite their brutality and shortcomings. These include important shifts at the international and local levels creating a feedback loop of inherent difficulty in deterring their rise. (1) Governance failure and inadequate political systems have led to substate nationalism and state fragility. There is a complete lack of confidence of different constituencies in the capacity of their governments to treat them fairly and equally. (2) Ungoverned spaces and peripheral marginalisation have given rise to the revolt from the margins as part of a revolution of frustrated expectations.[2] These spaces, where state institutions have limited reach and impact, experience social disengagement.[3] Their governments have done little to ensure heterogenous representation. (3) Increasingly the strength of local systems of authority (chiefs and community leaders) is creating sources of power and authority outside the state. They are regulated by their own set of rules and are not an extension of state power. Co-opting and integrating these forms of local power is key for insurgent governance. (4) Identity politics is fusing with ideology to produce an explosive set of ideational tools for mobilisation. Politics is becoming more localised with a 'tribal pull' of closed societies integrating dynamics of blood and soil.[4] The combination of marginalisation with ethnic, cultural, educational and religious stagnation, and the loss of unifying national visions is feeding new ways of thinking about the future. (5) The bulge of unemployed or disaffected cadres, civil servants and youths, a phenomenon linked to eschewed development priorities, is providing important recruiting grounds within disaffected constituencies searching for new forms of empowerment. (6) The experienced failures of an interconnected world to provide solutions to urgent issues such as rising inequality, refugee crises and climate change have led to solutions being sought outside of multinational fora. This has been a consequence of the rise of big power politics and the proxy warfare dynamics that feed these insurgencies. Finally, (7) these insurgencies are

internally sustainable given the ease of communication systems and logistics to supply sanctuary, recruits and funding as a result of globalisation.

These groups are being misdiagnosed by the tendency to define them through their actions, goals and methods employed, or by placing them within the framework of extremism. Understanding them is a first step to devising adequate policies. To do so requires a new framework that studies their internal dynamics in the form of a *rebel-system* analysis capturing their complexity and separating agency factors from exogenous influences of the conflict-systems within which they function. The *rebel-system* is an operational paradigm premised on understanding an insurgency as an *integrated system*. It distinguishes between the internal elements under the direct control of the leadership of insurgent movements (ideology, approach to civilians, leadership and organisation); and the external elements (demographics, government responses, access to resources, external patrons, among other factors) that the insurgent leadership cannot always control.[5] Viewing them as a system allows for an understanding of survivability, reproductive and transformative capacities during different stages of war and during peacetime. This kind of analysis aims to provide new perspectives to facilitate dialogue and political solutions in countries where such insurgencies operate.

Parallel states

Parallel states have a few distinguishing features that help an insurgency exercise effective control over a portion of state territory. The states these insurgencies create and govern vary significantly but some dynamics are worth mentioning. The rule of insurgents is over land as much as it is over people. Territorial control is crucial, but it requires inhabitants to populate the space and give rise to the parallel society. Social engineering is just as important as the outlining of a new political order. In addition, society influences the organisation of the state but does not take precedence over it. This differs and produces different challenges if insurgents occupy urban, peri-urban or rural areas with strong social organisation or functioning systems of informal authority. Governance in parallel states is driven by policy, identity, patronage and logistics. Insurgents devise a political program that may or may not reflect key values of its social base even as they employ strategies of patronage to deepen relations with local sources of authority. Governance in this way reveals the most fundamental organisational strengths and logistics capacity of these groups. Their access to resources, capacity to secure and develop different capital (financial, social and human) and their ability to absorb, process and disperse their resources in different areas are a defining structural element of governance.

The conflicts in Syria and Iraq have produced different forms of these insurgencies that have held or currently hold territory. They differ greatly in all the elements of their rebel-system and vary in terms of efficiency in

governing their 'liberated' areas. IS and the PYD continue to challenge the resolution of these conflicts. IS controlled over 11 million people at its peak in 2014 while the PYD governed over 5 million civilians in Western Syria.[6] The PYD is seeking a post-war political solution but is constrained by its external links, a weak ideological base with faltering levels of local legitimacy, and Kurdish rivalries threatening the idea of nationhood. Since the loss of its caliphate in 2016–2017 IS has had to adapt and re-emerge with a different strategy in Syria, Iraq and its provinces abroad. It has experienced mass decapitation of leaders, commanders and administrators and has lost important financial revenue sources. Both have suffered military defeats and lost territory; yet both reveal a level of resilience that will keep them engaged for several years. This section will not produce rebel-system analysis for these two groups but will rather briefly identify some features of their parallel states and governance strategies. The PYD and IS's governing experiences were pillared on very different organisational and symbolic imperatives. They have distinct theories of operation and therefore require different solutions.

To govern these insurgencies required stability – external and internal – in their territories. External stability relates to the ability to control territory without having to engage in combat from enemy forces to retake liberated areas. Governing in a transitory way under the threat of aerial bombardments changes governance. Internal stability relates to the capacity of these insurgencies to retain internal peace. Unified rule and security are key components of such stability as are access to courts and mechanisms to manage disputes among different communities. Both IS and the PYD carefully developed justice systems to regulate behaviour and mitigate internal conflict. IS ran two police forces, a morality police (*al-Hisba*) and a regular force (*al-Shurta al-Islamiya*). *Al-Hisba's* authority extended beyond civilians and combatants into keeping senior commanders and emirs in check. The judiciary also focused on correcting IS misconduct.[7] In the PYD's state, the justice system operates 'peace and consensus committees' mandated to deliver social justice and act as courts of first instance. At the top of the system is a justice parliament that has representation in each of the cantons and oversees the judicial system, instituting laws and new regulations. Order is maintained via a community police, the *Asayis* that operate as a civil defence force. These institutions cemented their control and pacified their diverse populations given the either strict and brutal ideology (IS) or their utopian ideology (PYD) both of which were not in line with the values and needs of all those they attempted to govern. Despite this, the provision of order and stability ground their governance.

Civilian populations cannot be controlled at all times. To govern parallel states, elements of consent and authority are crucial even while they balance different degrees of control and coercion. Without service delivery and safety to act as trade-offs for shortcoming in governance and coercion, insurgencies struggle to govern. The PYD has been efficient in the delivery of

services, a major source of legitimacy and organisational development, despite its relative isolation with the Turkish blockade and tense relations with the Iraqi Kurdistan Regional Government (KRG). Local level subsistence is regionally specific to each canton and coordinated through councils and sectoral cooperatives. Former state-owned lands have been distributed to the councils and organised into cooperatives, where 75% of property is community owned.[8] The healthcare system is coordinated by health assemblies and runs six hospitals in Rojava. Its biggest strength was its organisation and being responsive to particular needs. However, a group as well-funded, centralised and bureaucratised as IS, that held many organisational traits able to respond to civilian needs, faced several challenges. Its healthcare system was one of its worst performing areas. Its refusal to negotiate with international organisations to allow for foreign medical aid and strict rules imposed on female doctors paralysed the healthcare system that was already under strain by lack of medication, faltering electricity and lack of doctors. It did however run a well-planned war economy that had as much as $2 billion in assets, and was directed towards self-sustainability, maximising resources and securing large revenue streams. It imposed several taxes but also subsidised several services.[9]

Parallel states also in principle function in contrast to the state they oppose. They are embedded in the ideology that governs these groups as they attempt to enact change across society-state and society-society relations. There are symbolic and bureaucratic elements to this. The meteoric rise of IS revealed that, as an institution, the caliphate no longer remained a religious-government authority of the past but was a living idea that captured the imagination of many. It brought together a sense of nostalgic promise to correct the political order that had failed them and restore the just order of Islam.[10] It became a vehicle for salvation and a collective religious obligation.[11] In this sense the governance project was a carefully designed social and political engineering project. The parallel state of the PYD in Rojava has completely altered the way people govern themselves and relate to the state as an institution. Its political order stands in stark contrast to the Baathist regime in Damascus. Rojava is a concrete example of democratic confederalism that removes the 'state' as a necessary entity to govern society. It aims to become a transformative bottom-up governance model for a federated Syria that links society through people's assemblies, using a secular policy of decentralisation. The movement combines different contradictory nationalist, anti-nationalist, communist and multi-ethnic influences.[12] Any contradictions between governing practice and ideology can be corrected via strong propaganda strategies both of which these movements have.

Parallel states are also generally pillared along the organisation of one branch of the insurgency. Groups that have strong administrative branches that operate within the political organ are better placed to govern than groups that use their military hierarchy to structure governance. IS divided

the administration of its caliphate into different *Wilayats* (or statelets) and then sub-divided these into sectors. The governing structure was comprised of two pillars: Sharia administration (courts system, religious police and other law enforcement, education, health, tribal relations, Islamic outreach and Sharia institutes) and Muslim Services (service provision and infrastructure which included water treatment plants and power plants, bakeries and subsidised markets).[13.] Its structures were aimed at absolute control which together with its millenarian worldview had the objective of curbing any alternative thought, political pluralism and social organisation.[14] The PYD governs under the banner of the Movement for a Democratic Society (TEV-DEM), a six-party coalition that oversees the cantonal governance system of the Democratic Autonomous Administration (DAA). The DAA is divided into 22 executive councils equivalent to ministries with representatives at all levels (from the commune to the federate level). Decisions are conveyed up the system by two delegates (a man and a woman) at each level. Local councils include representatives of Kurdish political parties and non-Kurdish communities but are appointed by the PYD that maintains overall decision-making authority.[15] Both groups had bureaucratic capacity to govern along political structures that allowed them to separate their military wings from administrative power centres.

Ideology and political programs need to resonate with the values and needs of the people they govern. Both failed to achieve a cross-community following that cemented a wide and diverse constituency. The PYD currently retains control over large portions of Northern Syria and governs Kurdish areas, polyethnic areas where Kurds are a slim majority and areas were Kurds rule over Arab-majority towns. Rojava's Social Contract stipulates a multi-ethnic confederalist approach; yet many Arab, Syriac and Assyrian leaders and communities participate without adhering to its ideology.[16] It has struggled to sustain a political project without complete social adherence across communities, leading to a process of hegemonic control, assimilation and repression. The PYD has failed to harness supporters from non-Kurdish populations and failed to capitalise on the potentially unifying capacity of Kurdish nationalism. IS's doctrinal rigidity and brutality ostracised its diverse communities failing to create a unifying platform across territories. It has rallied support from small extremist groups across territories but has failed to secure a large civilian following. It did however persuade and indoctrinate supporters in Iraq guaranteeing loyalty even after its territorial demise while influencing the political thought of others that did not adhere to its ideology. Supporters in Mosul, for example, believe in achieving a Sunni Arab homeland governed by Sharia law; these have become non-negotiable scared values.[17] These nationalist sentiments may however localise it more and ground its organisation more concretely to specific territories.

Different strategies exist to link civilians to the state project. One important propaganda tool that allows for these insurgencies to alter the way their citizens think of themselves and their future is education. Some

groups carefully structure interventions in education, others don't have that capacity. The PYD has prioritised education as a revolutionary force. The curriculum includes education in Kurdish, Arabic and Syriac. By mid-2014 it had over 900 Kurdish teachers trained to teach Kurdish history, literature, women's science, democratic nation ideology and the history of assimilation.[18] The education system within IS's caliphate was also a propagation of its vision and an indoctrination tool. Several secular subjects that were considered illegitimate according to Sharia were removed from the curriculum, while group mythology was taught. Both these strategies of education have facilitated the extension of the groups' ideologies and the creation of supporters that because of their exposure at a young age are a new generation of cadres and combatants.

The manner in which IS and the PYD-YPG managed to control and direct each of these dynamics was a direct result of their leadership structures, ideological strength, organisational complexity and efficiency, and responsive policy towards civilians and their needs. The conflicts they operate in will continue to fluctuate between containment, asymmetric military confrontations and difficult political transitions. These insurgencies have added levels of protractability but have also deeply divided communities, tearing apart the social fabric of their countries, and in the process creating expectations of different political orders to restore the dignity of marginalised communities (even when as insurgents they failed to do so). They place civilians at the centre of this state-building endeavour and change the ways communities govern themselves during war. Any strategy devised to defeat or neutralise such groups will directly impact civilians and human security in greater ways.

Retooling international responses

Conflicts are complex in their causality, regulation and resolution.[19] Any negotiation or politico-military strategy begins with an understanding of the actors, their capacity and what they want to achieve. Incorrect explanations of the conflict will lead to dysfunctional conflict resolution processes. In fact, conflicts 'may be protracted, not necessarily or merely because of their inherent complexities, but because of the ways they have been initially defined, and because of the means employed to manage them'.[20] Furthermore, in addressing intractable conflicts several responses can be tailored to address a myriad of issues but without a clear understanding of what these responses add up to.[21] The main focus should remain on defining the conflict and its component parts correctly by mapping positions, interests, needs and fears. There is a need to seek (1) political solutions and (2) understand and address the shifts in authority and legitimacy that come from parallel states in differing degrees, which, in turn, creates the need to (3) think differently about the state and the pillars of governance. Responses need to be context-specific and actor specific. Multiple interventions can coexist, but

political solutions are necessary at every juncture. Governance arrangements need to focus on sustaining authority and legitimacy in whichever hybrid form they occur. Interventions therefore need to be transformative and focused on what the future will look like for these constituencies.

Political solutions

Several of these insurgencies are deemed as involving violent extremists, foreclosing political solutions for military responses. Long, asymmetrical and divisive wars have in the past experienced military responses to tackle these insurgencies and determine a political settlement. While the use of force may be necessary to stop ethnic cleansing, separate armed groups and ensure humanitarian space, these wars require political solutions that focus on a human security dimension. Insurgencies of this nature build their political legitimacy by creating their own duality and exclusionary identity which military strategies feed. Counterterrorism (CT) and Counterinsurgency (COIN) strategies both generalise the problem, and neither are transformative in the way that conflict transformation requires.[22] Labelling a conflict as comprising of violent extremist or terrorist groups risks 'pushing policy away from politics' and pursuing policy avenues that will delay resolving the issue.[23] Designating groups as terrorists may limit the movements' options, constraining efforts to de-escalate, shutting down potential avenues for dialogue and releasing them of the responsibility of good governance. It may also feed the notion of victimhood, collective punishment and humiliation that further entrench narratives of war, opposing visions of the future and the justification for continued violence.

Peace processes should therefore not be rendered second to military operations. Extremists and so-called spoilers need to be engaged with, despite the fears that in doing so they provide these groups with legitimacy, may undermine moderate politicians and may allow the space for them to regroup. This may require a conceptual shift by mediators and state actors into what compromises are possible. Some insurgent goals may seem unattainable through negotiations. However, goals shift overtime with engagement. More importantly these groups are locally embedded and grow through insurgent action aimed at exploiting local grievances that can be addressed through diplomatic action and negotiation. A systemic view of insurgencies divides the problem into different parts, corresponding to the component parts of the insurgency and the component parts of the conflict. Understanding how rooted certain insurgencies are with their 'people' is important for resolution purposes. Failing to address these specific nuances will most likely leave seeds of insurrection for other cycles of war and new insurgencies to exacerbate. The assessment of ideology provides insights into the groups coherence in translating aspirations into concrete political programs capable of fitting into political reform processes post-war. The systemic approach will allow for an understanding of the leadership's capacity

to keep a command stable through negotiations and sell difficult concessions to their support base, and their reproductive capacity to manage disputes at central and local levels. Organisationally it will allow an assessment of the resilience and experience of the political and administrative organs, shedding light on how each branch generates power and ensures survivability. The strength of the 'social contract' with civilian populations and the level of embeddedness with traditional structures of authority will facilitate an understanding of local conditions and layers of legitimacy that need accommodation. A systemic analysis also facilitates an understanding of which elements of these insurgencies have reached a critical mass level where addressing the initial root causes will not resolve these conflicts. By virtue of their development, these groups have generated entirely new factors in need of consideration and resolution.[24] Insight into the *rebel-system* will aid the design of different strategies.[25] It will provide an interpretive frame allowing one to identify entry points for appropriate and achievable objectives, which corresponds to Breekveldt and Kitzen's findings as mentioned in Chapter 5. The format future negotiations may take with these groups will entail an array of tools and strategies. Normative flexibility may be required to seek compromise so that political processes can be infused with ownership, credibility and a sense of fairness. Mediators will need to begin accommodating the contours of hybrid governance in areas with mixed authority and parallel systems. The strengthening of local authority capacity for inclusive and participatory governance is necessary to avoid the reinforcement of power structures that in the past excluded the values, and identities of conflict-affected communities.[26] Equipping local leaders, insurgent groups and community organisations with the necessary tools to 'govern in parallel' will remain riddled with legal, political and conceptual problems. Nevertheless, new forms of political transformation and state reform at the local level of diverse communities will need to be considered. Some groups may be equipped to provide for reformulated governance, others may not. The rebel-system will help determine those that can and those that can't.

Rethinking governance

International and regional responses continue to focus on the re-establishment of state authority and returning countries to their pre-war state. Because they have the *state* as the horizon, these tools are unresponsive to the objectives of insurgencies aiming to dislocate the state and transform political governance. Interventions that involve political and economic responses approach governance with a focus on the central state rather than understanding authority as a complex and multifaceted endeavour. Several large-scale international interventions further apply tested and modular approaches to state-building that disregard national and endogenous processes. Sub-national and local concerns are in these cases addressed through different interventions that ultimately strive to legitimise externality. Building legitimacy of the state by

excluding the communities that support these insurgencies is counterintuitive. Co-opting local elites and securing the local population to starve an insurgency of its support base may not be enough to undermine these insurgents. Rather, state-building is a political effort that needs to begin by generating mechanisms of power and authority.[27] It is a process of constant negotiation that can neither follow a prescribed path of 'best international practices', have a tight timeframe for implementation or be dependent on a static political authority. The new state and its institutions should emerge out of existing social forces, reflecting the interests and values on all sides of the conflict.

The creation and sustainability of hybrid political orders are not a new phenomenon. Political institutions of different natures and authority (customary, religious, civilian and institutional) have been combined with existing available institutions. These have blurred the delineation between the 'state' and informal' institutions as they combine, complement and borrow elements from each other. Hybrid political orders have several components that range from the restructuring of political power, security, to justice, education systems and other services. As a concept, it is neither state-centric, does not presuppose any particular arrangement or determine any level of effectiveness. It is open to dynamic change and does not lend it itself to particular social fields or types of informal/formal interactions. [28] However, hybrid governance arrangements need to begin considering the different forms of authority generated by parallel state-building insurgents. They represent major challenges to different post-conflict policy areas like democratisation, peacebuilding and state-building but nevertheless require new considerations.[29] Policies need to become more holistic, multi-layered, inclusive and localised.

Conclusion

Countries, populations and territories that experience the parallel government of these insurgencies go through significant adjustments in the realities of their human and physical geography. Interventions need to take into consideration several factors. First, conflicts need to be correctly defined as do the actors engaged in them by understanding what drives them and what component parts provide reinforcing dynamics of sustained enmity, fear and distrust. Second, engagements of the different sides need to occur at any point regardless of the ripeness of the conflict. The urgency of engagement relates to the human security dimensions of such wars and the timeframe it will take to deescalate the conflict. Third, multiple forms of intervention can coexist including military options but should always be accompanied with integrated and sustained political interventions. These interventions need to be appropriate to the unique aspects of each war. Fourth, talking to extremists on all sides is vitally important. Fifth, context-specific resolution processes need to be prioritised over 'best -practices'. Existential

threats, cultural diversity, differing political ideologies and imagined orders require tailored responses. Governance arrangements that include differing levels of hybridity need to be brought into frameworks for peace negotiations. Lastly, the resolution of these conflicts also needs to be connected to transformative and constructive change processes to counter destructive patterns. The focus is on what the future will look like.

The residual impact of these wars, and the insurgencies fighting them, will place greater pressure on state sovereignty and the responses required of heterogenous nation-states in dealing with their diverse populations. Narrow responses to these insurgencies will only increase the likelihood that their resurgence will become more extreme each time as either violent jihadism, separatist nationalism, reformist sub-nationalism or utopian extremism. Governance will need to take on different forms to adapt to the challenges ahead and the changing environment, which may lead to more localised organic and transnational societies. Analysts and political leaders globally would do well to begin thinking flexibly on how to accommodate such shifts and what they will mean for the international order. The hybridisation of government, where key state functions are transferred to non-state actors, will increasingly challenge this order. Demands for devolution of power and assertive minority demands for control of their resources, political systems and regional engagements will increasingly elevate the local level and certain peripheries to the forefront of politics. Power will as a result be dispersed across borders, unconfined to existing nation-states and increasingly networked to compete with established internationally regulated systems. These insurgencies will not catalyse these shifts but are influencing changes and will benefit from the inability of states to shape outcomes in the international order.

Notes

1 Hew Strachan, 'The Changing Character of War', Europaeum Lecture (Geneva: Graduate Institute of International Relations, 2006).
2 Paul Rogers, Irregular War: The New Threat from the Margins (London: I.B. Tauris, 2017), 12.
3 Angel Rabassa, Steven Boraz, Peter Chalk, Kim Cragin, Theodore Karasik, Jennifer Moroney, Kevin O'Brien, and Kevin John Peters, Ungoverned Territories. Understanding and Reducing Terrorism Risks (Santa Monica, CA: RAND, 2007).
4 Francis Fukuyama, 'Why Liberal Democracy Is in Trouble', National Public Radio, 4th April 2017.
5 Assessing leadership requires an understanding of the compromises and balances necessary to keep a command unified in both flat-hierarchical structures and vertical forms of collective command. Leaders and their second-tier commanders are key in maintaining cohesion, mobilisation and growth but different structures and dynamics will influence ideological and organisational forms. Leaders are also instrumental in tailoring responses to survive critical junctures, and understanding which balances are required. Ideology and political programs are assessed from the perspective of their capacity to mobilise and order grievances in effective ways. They need to justify a war of 'liberation'

to particular constituencies and tailor messages pragmatically for internal and external audiences. Organisational aspects are defined from the perspective of the complexity of different organs and how each branch relates to the other; it involves structuring power, coordinating structures and devolving power to different areas and leaders. Approach to civilians relates to the capacity to use constraints on the ground to redirect local conditions in support of the war; the use of existing systems of authority (chiefs, tribal leaders, etc.); the ability to educate and indoctrinate civilians into constituents; and the willingness to allow civilians the space to define relations with the parallel state. See, for instance, Seth Jones, Waging Insurgent Warfare Lessons from the Vietcong to the Islamic State (New York: Oxford University Press, 2017), John MacKinlay, 'Globalisation and Insurgency', The Adelphi Papers 42:352 (2002), Bard O'Neill, Insurgency and Terrorism: Inside Modern Revolutionary Warfare (Washington, DC: Brassey's, 1990), David Kilcullen, 'Counterinsurgency Redux', Survival 48:4 (2006), 111–130, David Kilcullen, 'Countering Global Insurgency', Small Wars Journal, 30 November 2004; Nathan Leites and Charles Wolf, Rebellion and Authority: An Analytical Essay on Insurgent Conflicts (Santa Monica, CA: RAND, 1970).

6 Seth Jones, James Dobbins, Daniel Byman, Christopher Chivvis, Ben Connable, Jeffrey Martini, Eric Robinson, and Nathan Chandler, Rolling Back the Islamic State (Santa Monica, CA: RAND, 2017), Fritz Lodge, 'The Promises and Perils of Syrian Kurdistan', Cipherbrief, 22 September 2017.

7 Mona Alami, 'ISIS's Governance Crisis (Part II): Social Services', Atlantic Council, 24 December 2014.

8 Matthew Moberg, 'Nation-building in Rojava: Participatory Democracy Amidst the Syrian Civil War', Pathways to Peace and Security 2:51 (2016), 15–36.

9 Hassan Haniyeh, 'Daesh's Organizational Structure', Al Jazeera Center for Studies, 4 December 2014.

10 Ofir Winter, 'The Islamic Caliphate: A Controversial Consensus', in Yoram Schweitzer, and Omer Einav eds., The Islamic State: How Viable Is It? (Tel Aviv: The Institute for National Security Studies, 2016), 27.

11 Graeme Wood, 'What ISIS Really Wants', The Atlantic, March 2015, Fawaz Gerges, 'The World According to ISIS', Foreign Policy Journal, 18 March 2016.

12 Moberg, 'Nation-building in Rojava'.

13 Charles Caris and Samuel Reynolds, ISIS Governance in Syria (Washington, DC: Institute for the Study of War, 2014).

14 Gerges, 'The World According to ISIS'.

15 International Crisis Group, 'Flight of Icarus? The PYD's Precarious Rise in Syria', Middle East Report 151 (2014).

16 Ibid.

17 Scott Atran, Scott, Hoshang Waziri, Angel Gomez, Hammad Sheikh, Lucia Lopez-Rodriguez, Charles Rogan, and Richard Davis, 'The Islamic State's Lingering Legacy among Young Men from the Mosul Area', CTC Sentinel 11:4 (2018), 15–22.

18 Michael Knapp, Anja Flach, and Ercan Ayboga, Revolution in Rojava: Democratic Autonomy and Women's Liberation in Syrian Kurdistan (London: Pluto Press, 2016).

19 Marianne Heiberg, Brendan O'Leary, and John Tirman, eds., Terror, Insurgency and the State. Ending Protracted Conflicts (Philadelphia: University of Pennsylvania Press, 2007), 10.

20 John Burton, Resolving Deep-Rooted Conflicts (Lanham, MD: University Press of America, 1987), 21.

21 John Paul Lederach, 'Conflict Transformation', Beyond Intractability, October 2003 .

22 Abu-Nimer, Mohammed, 'Alternative Approaches to Transforming Violent Extremism. The case of Islamic Peace and Interreligious Peacebuilding', in Transformative Approaches to Violent Extremism, Berghof Handbook Dialogue Series no. 13, eds. Beatrix Austin and Hans Giessman (Berlin: Berghof Foundation, 2018).
23 International Crisis Group, 'Exploiting Disorder: Al-Qaeda and the Islamic State', Special Report 1 (2016).
24 Kilcullen, David, 'Countering Global Insurgency'.
25 Understanding the component parts of each rebellion is merely one element of a larger strategy to ends wars and build peace. Responses also need to be provided to the structural issues that led to their emergence and the proxy dynamics and regional rivalries that help sustain them. These other components fall outside the remit of this chapter.
26 Ashley South, '"Hybrid Governance" and the Politics of Legitimacy in the Myanmar Peace Process', Journal of Contemporary Asia 48:1 (2018), 1–17.
27 Marina Ottaway, 'Rebuilding State Institutions in Collapsed States', Development and Change 33:5 (2002), 1001–1023.
28 Maren Kraushaar and David Lambach, 'Hybrid Political Orders: The Added Value of a New Concept', The Australian Centre for Conflict and Peace Studies Occasional Paper 14 (2009).
29 Kraushaar and Lambach, 'Hybrid Political Orders'.

References

Abu-Nimer, Mohammed, 'Alternative Approaches to Transforming Violent Extremism. The Case of Islamic Peace and Interreligious Peacebuilding', in Austin, Beatrix, Giessman, Hans eds., 'Transformative Approaches to Violent Extremism', *Berghof Handbook Dialogue Series no. 13* (2018), 1–21.

Alami, Mona, 'ISIS's Governance Crisis (Part II): Social Services', *Atlantic Council*, December 2014.

Atran, Scott, Waziri, Hoshang, Gomez, Angel, Sheikh, Hammad, Lopez-Rodriguez, Lucia, Rogan, Charles, and Davis, Richard, 'The Islamic State's Lingering Legacy among Young Men from the Mosul Area', *CTC Sentinel* 11:4 (2018), 15-–22.

Burton, John, *Resolving Deep-Rooted Conflicts* (Lanham, MD: University Press of America, 1987).

Caris, Charles, and Reynolds, Samuel, *ISIS Governance in Syria* (Washington, DC: Institute for the Study of War, 2014).

Chandler, David, 'Back to the Future? The Limits of Neo-Wilsonian Ideals of Exporting Democracy', *Review of International Studies* 32:2 (2006), 475–494.

Gerges, Fawaz, 'The World According to ISIS', *Foreign Policy Journal*, 18 March 2016.

Haniyeh, Hassan, 'Daesh's Organizational Structure', *Al Jazeera Center for Studies*, 4 December 2014.

Heiberg, Marianne, O'Leary, Brendan, and Tirman, John, eds., *Terror, Insurgency and the State. Ending Protracted Conflicts* (Philadelphia: University of Pennsylvania Press, 2007).

International Crisis Group, 'Exploiting Disorder: Al-Qaeda and the Islamic State', *Special Report* 1 (2016).

International Crisis Group, 'Flight of Icarus? The PYD's Precarious Rise in Syria', *Middle East Report* 151 (2014).

Jones, Seth, *Waging Insurgent Warfare Lessons from the Vietcong to the Islamic State* (New York: Oxford University Press, 2017).

Kilcullen, David, 'Countering Global Insurgency', *Small Wars Journal*, 30 November 2004.

Kilcullen, 'Counterinsurgency Redux', *Survival* 48:4 (2006), 111–130.

Knapp, Michael, Flach, Anja, Ayboga, Ercan, *Revolution in Rojava: Democratic Autonomy and Women's Liberation in Syrian Kurdistan* (London: Pluto Press, 2016).

Kraushaar, Maren, Lambach, David, 'Hybrid Political Orders: The Added Value of a New Concept', *The Australian Centre for Conflict and Peace Studies Occasional Paper* 14 (2009).

Lederach, John Paul, 'Conflict Transformation', *Beyond Intractability*, October 2003.

Leites, Nathan, and Wolf, Charles, *Rebellion and Authority: An Analytical Essay on Insurgent Conflicts* (Santa Monica, CA: RAND, 1970).

MacKinlay, John 'Globalisation and Insurgency', *The Adelphi Papers* 42:352 (2002).

Moberg, M., 'Nation-building in Rojava: Participatory Democracy Amidst the Syrian Civil War', *Pathways to Peace and Security* 2:51 (2016), 15–36.

O'Neill, Bard, *Insurgency and Terrorism. Inside Modern Revolutionary Warfare* (Washington, DC: Brassey's, 1990).

Ottaway, Marina, 'Rebuilding State Institutions in Collapsed States', *Development and Change* 33:5 (2002), 1001–1023.

Rabasa, Angel, Boraz, Steven, Chalk, Peter, Cragin, Kim, Karasik, Theodore, Moroney, Jennifer; O'Brien, Kevin, and Peters, John, *Ungoverned Territories. Understanding and Reducing Terrorism Risks* (Santa Monica, CA: RAND, 2007).

Rogers, Paul, *Irregular War: The New Threat from the Margins* (London: I.B. Tauris, 2017).

Schweitzer, Yoram, and Einav, Omer, eds., *The Islamic State: How Viable Is It?* (Tel Aviv: The Institute for National Security Studies, 2016).

South, Ashley, '"Hybrid Governance" and the Politics of Legitimacy in the Myanmar Peace Process', *Journal of Contemporary Asia* 48:1 (2018), 1–17.

Strachan, Hew, The Changing Character of War, *Europaeum Lecture* (Geneva: Graduate Institute of International Relations, 2006).

Winter, Ofir, 'The Islamic Caliphate: A Controversial Consensus', in Schweitzer, Yoram, Einav, Omer eds., *The Islamic State: How Viable Is It?* (Tel Aviv: The Institute for National Security Studies, 2016), 27–36.

Wood, Graeme, 'What ISIS Really Wants', *The Atlantic*, March 2015.

11 Security force assistance as a preferred form of 21st century warfare

The unconventional becomes the conventional

Jahara Matisek and Ivor Wiltenburg

Introduction

Notions of conventional military warfare, best defined through combined arms manoeuvre, have been the exception rather than the norm in the 21st century. Preoccupying most militaries has been the unconventional military mission of providing security assistance to weak and failing states. Despite substantial resources being committed to such endeavours by the United States, North Atlantic Treaty Organization (NATO) member states, and the European Union, there are very few success stories. The recent surge of security force assistance (SFA) missions by Western states, to train, advise, and assist (TAA) host-nation militaries and militias in weak states, is due to a lack of political willpower. Averse to committing large numbers of forces for fighting insurgencies or terrorists in insecure, instable, and underdeveloped countries, SFA and TAA-type operations are initiated to limit costs and casualties. However, this risk-averse strategy has associated externalities. Special operations forces (SOF), who have historically been tasked with unconventional military duties of indirect action, such as assisting weak state armies and pro-Western rebels, are overstretched. Hence, the 'unconventional' duty of SFA is being burden-shifted to conventional military units to alleviate the strain on SOF units constantly deploying to advise foreign forces.

This chapter first sketches the historical context of military assistance (MA) missions, which have been a mainstay of international politics, more so over the last 200 years. Such context clarifies how SFA has become a common tool for responding to state weakness, insurgency, and terrorism. Second, we show how SFA has increasingly become the newly institutionalised way of war for the West. Third, we illustrate the allure and challenges of modern SFA becoming normalised and bureaucratised in the West. However, the SFA mission is a highly personalised and culturally sensitive activity, something conventional military units are not organised or designed to do. This is because weak states have a fragmented political context where state monopoly of violence is contested due to the presence of numerous security actors (e.g. militias, insurgents, terrorists, criminals).[1]

The paradox inherent with most modern militaries is they have increasingly taken a bureaucratised (i.e. rational-legal) approach to warfare. Such a rigid Weberian approach to unconventional warfare (i.e. SFA) is problematic in a fragile state because the societal and political system lacks bureaucratic institutions and civil war has often personalised the violence. Flexible informal institutions based on traditions and charisma inform the organisation of governance, power, and legitimacy, each emphasising personal relationships.[2] In this context, it is near-impossible to successfully implement the current bureaucratic and impersonal approach to SFA, because the logic of politics in a weak/collapsed state is controlled by powerful informal elites that perceive effective bureaucratic institutions as threatening their authority. Despite such failings, this chapter ultimately concludes that SFA is here to stay for the foreseeable future due to its cheapness, low-risk, increasing pressure of great power competition, and the complications associated with state failure (e.g. disruptive refugee flows to Western countries).

The evolution of military assistance

Since the Peloponnesian War, the concept of a stronger state lending military aid, assistance, and training to a weaker state to make their army stronger has been a tool of exercising power. However, industrialisation alongside the rise of colonialism changed the depth and scale of security assistance missions. Much of this originally rested on a colonising power creating a friendly puppet regime with a trustworthy police and loyal army that reflected the values and institutions of the colonising force. Industrial warfare intensified this process in the 19th and 20th century through increased specialisation and bureaucratisation of organisations for efficient warfare. However, during the post-colonial period this hitherto efficient process of co-option could no longer be realised. Nonetheless, the TAA approach to indigenous forces proved to be an indispensable military task, in improving the effectiveness of militias, partisans, and resistance fighters fighting against a common enemy. As these indirect operations were conducted frequently behind enemy lines, it became part of the special operations warfare branch, and as such included in the described tasks of SOF.[3]

While 'special military units' existed prior – there are many documented uses of 'Special Forces' being created and employed throughout history – the emergence of modern SOF occurred during the Second World War. The Cold War and various anti-colonial movements led to SOF growing in size and scope, becoming permanent fixtures in the branches of many industrialised armed forces.[4] The emergence and increased prevalence of small wars during the Cold War era gave civilians a more predominant role in internal conflicts – instead of the uniformed adversaries Western armies trained for.[5] Civil wars are best defined as a 'struggle against intimate enemies: indeed, against those who should never have been conceived of as enemies at all'.[6] Traditional large-scale Western warfare is highly contradictory to such a

'war amongst the people', in which granular intelligence and the selective employment of discriminate violence are more effective than overwhelming firepower.[7]

Doctrine development on how to conduct unconventional warfare began early in the 20th century such as the U.S. *Small Wars Manual* based on the experience of Marines fighting in the so-called Banana Wars (1898–1934).[8] T.E. Lawrence's emphasis on how to work with local armed groups was similar, but with specific focus on fostering personal relationships.[9] Western MA missions, using small units, were especially important in peripheral areas (e.g. Africa, the Arab Peninsula, Asia) during the First World War and Second World War, because the bulk of forces were deployed for conventional military assaults in Europe and Asia.

The end of the Second World War brought a new threat to the West: communism. This new ideological threat – projected by the full weight and force of the Soviet Union – became problematic for the United States and Western Europe. Quite quickly, SOF units and special advisory groups were enlarged to train up anti-communist rebels in various regions and to develop the armed forces in Greece, South Korea, and Turkey.[10] As best envisioned by U.S. General James A. Van Fleet in 1954, he saw MA as engaging foreign security challenges cheaply, fielding '25 divisions at the cost of one'.[11]

Needing to defeat an internal communist threat created a subset of unconventional warfare. Doctrinally known as Foreign Internal Defense (FID) in the United States, it was a defining pillar of American efforts in the Vietnam War and elsewhere. In fact, during the Cold War at least 55 documented countries received American military (and/or paramilitary) assistance for the FID mission.[12] Similarly, the decolonisation era led to European powers (e.g. United Kingdom, France, the Netherlands, Belgium, Portugal) sometimes waging incredibly brutal counterinsurgencies (e.g. Algeria, Dutch East Indies, Malaya), sometimes with the help of local proxy forces, to only still eventually lose their colonies.[13] Even after their independence, European MA efforts continued to former colonies for supporting their fight against local irregulars and garrisoning against communist influence.

After the Cold War ended, the necessity for foreign powers to employ SOF and general MA missions substantially decreased. As a consequence it became readily apparent in the 1990s that many states had only been able to subsist through aid programs from the Western and/or Eastern bloc. Many of these fragile states were dependent on being subsidised by foreign economic assistance and MA.[14] This structural change in the international system, combined with numerous unresolved political grievances in weak states, provided the conditions for new forms of civil wars to emerge. As best elucidated by Mary Kaldor, these 'new wars' were defined by four principles: (1) violence between networks of state and non-state actors, (2) identity politics driving violence, (3) the pursuit of political control through violent means, and (4) predatory ways of financing internal warfighting.[15] Subsequently, many governments collapsed, leading to ungoverned state-less spaces that

were exploited by various armed actors, be it for ideological, political, and/or financial gain.

In this environment, Western states attempt to mitigate the effects of these failed states on their own security, enabling local forces to fight for common goals. This effectively externalises the burden of warfare to a local agent, in what has been described as 'surrogate warfare'.[16] In a similar vein, the increased strategic distance between the belligerents by utilising proxies, but also stand-off weapon systems, has led to the use of the 'remote warfare' moniker.[17] Since 2007, SFA is the most common phrase used, as both the United States and NATO switched to this term to describe the training, advising, and assisting efforts in their respective doctrines.

Emphasising military assistance in the era of terrorism

The terrorist attacks of 9/11 and similarly inspired attacks across Europe after 2001 provided a new imperative for the West to deal with weak states, which was explicitly identified as a national interest in the Bush Administration's 2002 *National Security Strategy* and 2003 *European Security Strategy*.[18] The American-led invasions of Afghanistan (2001) and Iraq (2003), and their subsequent insurgencies, brought to the forefront the importance of creating stable and effective host-nation security forces. However, by late 2005 it was clear that American-led training of Afghan and Iraqi security forces was not working as these forces were unable to provide safety, security, or hold their own against insurgents. This was an indictment against the U.S. military and its flawed approach of trying to create new military institutions in these two countries. It also illustrated blindness to the lessons learned from over a century of American MA missions. Thus, the Joint Center for International Security Force Assistance (JCISFA) was created by the Secretary of Defense in April 2006 'to develop integrated tactics, techniques, and procedures (TTPs)' and 'institutionalize lessons and best practices from SFA operations' to better assist partner 'security forces during stability, security, transition, and reconstruction operations'.[19]

The development of such doctrine and the desire to train up host-nation security forces more efficiently throughout the Middle East and Africa – alongside the operational strain on SOF units – has driven the United States and United Kingdom to create specialised conventional military units to deliver SFA. The biggest advocate, Army Chief of Staff General Mark Milley, spearheaded the creation of six American Security Force Assistance Brigades (SFABs) in 2018.[20] Comparably, the British *Army 2020* white paper signalled the establishment of a Specialised Infantry Group (SIG) with four Specialised Infantry Battalions (SIBs) dedicated to the mission of SFA.[21]

Following suit, the NATO Security Force Assistance Centre of Excellence (NATO SFA COE) was established in 2019. The NATO SFA COE is formally tied to supporting the NRDC-ITA (NATO Rapid Deployable Corps – Italy), a multinational fighting force that has increasingly been relied upon to

provide SFA, like an SFAB or SIG. These types of conventional units being created to perform SFA reflect a shift towards a 21st-century era of trying to build capable army and police units in weak states. This increasingly points to the preferred low-risk way of war. Indeed, the safety of SFA personnel is regularly put on a premium instead of the success of the operation. For instance, an Italian colonel in 2019 describing how SFA can work best argued that 'Force Protection is ALWAYS the highest priority [sic]'.[22] However, his assessment undermines Clausewitzian notions of SFA being used towards political objectives beneficial to Western governments, further indicating a shift in the preferred way of war for the West.

The Western way of war

One of the first scholars to suggest there being a 'Way of War' was Russell Weigley. Looking at the historical American approach to war, Weigley noted how the United States evolved from a strategy of attrition to an annihilation approach. However, when nuclear weapons emerged, Weigley observed how this had radically changed the calculus of war making, because attempting to annihilate an enemy would likely result in mutually assured destruction via a nuclear response.[23] Thus, wars in the atomic age became a balancing act of limited war (e.g. unconventional warfare) in trying to pursue political objectives without reaching the tip of nuclear war, nullifying – as Weigley viewed it in Vietnam – the possibility of achieving a decisive victory. Following the failures of Vietnam, U.S. and other Western military leaders purposefully purged the lessons of Vietnam, by investing in technology and firepower, in pursuit of the next conventional war.[24]

The overwhelming defeat of Iraq in 1991 during the Persian Gulf War, the success of the 78-day air war against Yugoslavia (1999), and the rapid defeats of the armed forces of Afghanistan (2001) and Iraq (2003) provided a new lens in which to believe that a newly efficient way of war existed for the West. Leading the charge was Max Boot, who contended in 2003 that these quick and successful wars were a new way of war because technology had enabled a revolution in military affairs (RMA), whereby precision airstrikes could eliminate most adversary forces with little to no ground troops.[25] Stephen Biddle branded this new model of airpower and small SOF teams as the 'Afghan model', with 'indigenous allies' enabled without deploying large numbers of conventional ground forces.[26] However, after spending hundreds of billions of dollars on building and training Afghan and Iraqi security forces, they remain militarily ineffective.[27] The United States and allies had essentially created *Fabergé Egg* armies in Afghanistan and Iraq: expensive, but easily broken by insurgents.[28]

While there are some perils in discussing a specific Western way of war, much of the literature has trended towards some level of agreements about certain ways of fighting in the West compared to other societies and civilisations. One of the proponents of there being a Western way of war – and it

being superior to others – is Victor Davis Hanson. Hanson's seminal book, *Carnage and Culture*, pushes back against notions of geography and technology making one military better than another, contending that specific Western cultural traits (e.g. personal freedoms, citizen armies, group discipline with individual initiative encouraged) created effective militaries because they developed distinctive and innovative military cultures not bound to ritual, tradition, and religion.[29] This translated into strategies of annihilation for the West, whereas other societies typically pursued war to reach political settlements. The impersonalised Western approach to warfare makes it institutionally effective because of the way it is rationalised: overcoming traditional societal norms that can interfere with combat operations. However, for SFA to be effective, cultural context and personal relations need to be established over the long-term.[30] As noted by David Ucko, 'the U.S. government remains seriously ill-equipped for the task of countering irregular threats… and its problematic search for lower cost and lower risk ways of combating terrorism' is leading towards a preference for conventional units to conduct SFA missions.[31]

The creation of American SFABs and the British SIG to conventionally conduct SFA is not a radical idea in the normalisation of this once unconventional military duty. In fact, the NRDC-ITA has performed MA missions to 10 countries since 2001, with SFA only formally being codified into its activities in 2017.[32] Moreover, the EU first began SFA missions in 2010 in an attempt to rebuild the security forces of Somalia to support a newly formed government in Mogadishu to repel al-Shabaab. These EU-organised programs, known as European Union Training Missions (EUTMs), first began in Somalia (2010-Present), with other EUTMs providing SFA to the armed forces of Mali (2013-Present) and Central African Republic (2016-Present). Each of these internationalised military interventions into a civil war is a product of the current 21st-century international system, which perceives global interconnectedness as being endangered by a failed state, requiring intervention.[33] SFA is increasingly a greater component of trying to bring stability through the imposition of Westernised military institutions and various other forms of bureaucratised institutions that are remarkably different to how elites and citizens informally operate and conduct politics.[34] These rationalised attempts at SFA, however, involve 'trying to impose a merit-based, technologically savvy, equipment-intensive approach onto societies where relationships and social standing have a heavy bearing on organizational behaviour', which likely means these Western endeavours are dubious to produce effective militaries in their image.[35] Still, using SFA as a foreign policy tool is an enticing option for Western governments for various reasons.

The allure of SFA

SFA is appealing for several political reasons. First, it is perceived as a low-risk and economical way of addressing insurgency and terrorism in

certain regions, without committing large numbers of troops. Second, the tailored mission scope of SFA may only require a dozen advisors. With small numbers, SFA operations offer a non-militarised narrative of supporting local forces to provide security. Third, SFA enables coalition operations, as supporting local security institutions can be shared amongst coalition partners. Examples include the UN authorised International Security Assistance Force (ISAF) in Afghanistan and the Capacity Building Mission in Iraq (CBMI). Many small states, for the purposes of demonstrating resolve and loyalty to the United States, make meaningful troop contributions to SFA missions.[36] In fact, since the end of ISAF in 2014, the NATO-led Resolute Support Mission has transitioned into an explicit SFA mission, averaging about 17,000 troops, of which the United States has provided half the personnel, with 38 countries combining their forces to provide the other half.[37]

The Obama Administration, believing it would yield benefits to the United States and allies, adopted the doctrinal employment of SFA.[38] In 2009, Secretary of Defense Robert Gates stated the United States would use indirect approaches for security challenges wherever possible; building the capacity of partners was as important (or even more so) than U.S. troops doing the actual fighting.[39] This policy change was mainly a consequence of the U.S. Army and SOF being operationally strained – resulting in the need to address security challenges in an alternative fashion – in tandem with procuring costly new assets for great power competition. With fewer resources to conduct counterinsurgency (COIN) and counterterrorism (CT) operations across the Middle East and Africa, a transition to SFA was only logical to reduce troop commitments.

The rationale for smaller states is somewhat different. SFA participation allows small states to show support to their hegemonic ally, thereby legitimising foreign military interventions by broadening the international coalition, albeit still at a low-cost in the perception of domestic audiences.[40] However, changing perceptions of America's role in international affairs are making it increasingly difficult for allies to lend support.[41] Concerns of being implicated in an open-ended war might lead to some European capitals being suspicious of American-led aims of SFA.[42] Yet, for many small states SFA provides a 'non-combat' narrative in symbolically supporting internationalised state-building efforts in a weak state. Finally, SFA is perceived as cheap and less risky, both politically as well as physically, and TAA tasks are fungible making it easy for coalitions to adapt when members withdraw advisors.[43]

The challenges of SFA

With SFA being attractive to many states, successes have been elusive. Besides South Vietnam during the Cold War, on-going SFA efforts in Afghanistan, Iraq, Mali, Somalia, and many others appear to be failures.[44] A brief survey of SFA literature indicates several trends such as lack of success due to erroneous policy decisions, an overly technical approach, lack of

absorptive capacity by recipients, or the improper, illegal, or immoral use of the received SFA.[45] Indeed, providing SFA has shown to have a correlation with *coups d'état*, increased political violence, and domestic repression.[46]

Two decades in, the brittle forces of Afghanistan and Iraq have been unable to stand on their own. The ineffective Iraqi army collapsed in 2014 due to bad leadership and sectarian divisions, as evidenced by the easy capture of Mosul by a small group of Islamic State fighters.[47] Moreover, the Afghan army has been unable to overcome corruption and ethnic and tribal divisions. This has led to the Taliban controlling more territory in 2020 than they have since 2002. Such systemic issues seem unsolvable for the foreseeable future, making the prospect of 'winning' in each country only possible if the U.S.-led international community were to station over 100,000 troops in each country, much like the United States did with post-Second World War Germany, Italy, and Japan. Albeit, the United States was fortunate with these three countries possessing some level of Weberian bureaucratised institutions.

One of the other challenges encountered is a lack of absorptive capacity, with either individuals or institutions. Weak governments – either due to lack of willpower, capacity, and/or incompetence – struggle with integrating SFA. Specifically, many studies identify a partner's limited absorptive capacity as an obstacle to military effectiveness and institution building.[48] An example is the Somali government, which lacks the political willpower and capacity to engage in necessary reforms. No national-level official security force can protect Somalia writ large, as clan politics prevent international attempts at formalising effective institutions in Somalia.[49] This suggests a need to engage in a hybrid approach to SFA in these contexts, working towards building upon the localised ways in which authority and power are constructed, focussing more on peacebuilding than military power.[50] Creating hybrid security institutions that reflect political realities such as an oligopoly of violence would ensure some modicum of institutionalised buy-in from elites. Attempting to impose a Weberian model that artificially monopolises violence will likely prove more disruptive, undermining stability and hindering a democratic transition.[51]

A final important factor regarding successful SFA-provision is the mitigation of antagonistic external actors. This occurs when SFA efforts are 'spoiled' by third-party actors who attempt to stymie the building up of a host-nation military, by supporting insurgents.[52] Furthermore, as the presence of a SFA force does not provide any deterrence due to the lack of integral combat power, a small deployment of trainers to an area influenced by antagonistic third-party actors could be counterproductive as it exposes lightly armed and/or unarmed forces.

The shift from special forces towards conventional troops

SFA-type activities are termed MA in NATO SOF doctrine, as it has been historically a SOF task. Besides special reconnaissance and direct action, MA is indeed one of the main tasks for NATO SOF.[53] However, since

the interventions in Iraq and Afghanistan, troops from regular infantry battalions have been increasingly tasked to perform SFA. In Afghanistan, conventional coalition forces were used to staff the Operational Mentoring and Liaison Teams, which were attached to Afghan army units. Similar efforts occurred with the CBMI, with conventional troops assigned to Iraqi units. The increased need for senior non-commissioned officers and officers to provide TAA to foreign militaries has resulted in niche units such as Americans SFABs and British SIG. In smaller states, few organisational changes have been made to accommodate for the increased operational need for SFA advisors, but small states have nonetheless contributed significantly to these SFA-type operations by parsing regular units for deployable SFA units.[54] These organisational adaptations might indicate that SFA is a new concept, although historical antecedents indicate otherwise.

The former American SOF approach to 'provide advice, training and assistance to indigenous resistance organizations already in existence' has changed.[55] SFA is not limited to either light infantry or rebel forces; it has broadened to armoured warfare, artillery, and air forces. SOF personnel, although sometimes having prior experiences in these types of regular warfare, are not ideally suited to developing regular formations, because SOF personnel generally lack staff and logistical experience. Thus, regular army personnel find themselves increasingly in an advisory role. Still, for many states providing SFA, these new tasks have not been properly integrated into doctrines or organisational planning. For instance, a *Special Inspector General for Afghanistan Reconstruction* report indicated that SFABs lacked the necessary personnel to train and deploy properly for their SFA mission in Afghanistan, struggling to advise Afghan units.[56] As relayed in an interview with one SFAB officer, the U.S. Army is so (re)focused on conventional warfare that SFABs are treated as an afterthought. SFABs do not receive the necessary support and resources, lacking a broader strategy for providing SFA outside of Afghanistan, such as in Africa, and risk-aversion (i.e. protecting SFAB personnel) limits interaction with the armies they are supposed to train.[57]

Conclusion

The interventions (and post-stability operations) in Afghanistan and Iraq are failures. Military units providing SFA under risk-averse conditions contradict the fundamentals of the seminal *U.S. Army/Marine Corps Counterinsurgency Field Manual*, which highlights that 'ultimate success in COIN is gained by protecting the populace, not the COIN force'.[58] This speaks volumes to the various problems of an interloping force conducting COIN/CT operations, while juggling the TAA mission alongside nation- and state-building.

The number of casualties and high costs from the occupations of Afghanistan and Iraq have led Western aversions to large-scale foreign military interventions.[59] This sentiment has translated into limited military interventions via

SFA. Smaller missions with a distinct focus on an indirect approach involving local security forces have become more common. These TAA missions concentrate on enabling foreign security forces to achieve common security goals, leading to descriptions like 'surrogate' or 'remote' warfare.

Besides the shift from large interventions to smaller interventions via SFA, another trend is discernible. Although war is elementally a human endeavour, the bureaucratisation and modernisation of warfighting have increasingly made it impersonal. Close quarter combat and war amongst the people – a mainstay of fighting for millennia – is now increasingly considered to be avoided or unconventional. Conversely, conventional warfare has become more 'distant' through the increased use of stand-off precision weaponry, long-range direct firing platforms, and drone warfare. As 'unconventional warfare' has increased in occurrence since the beginning of the 21st century, epitomised by large counterinsurgencies in Afghanistan and Iraq, but also in Mali, Syria, and Ukraine, SOF units are increasingly stretched thin in providing all aspects of unconventional warfare to contemporary conflicts. This has resulted in conventional military forces filling the SFA gap. Such ad hoc operations have increasingly been institutionalised in the West, with SFABs and the SIG. These trends are indicative of the normalisation and bureaucratisation of SFA as a modern Western way of warfare. Western capitals prefer local proxies to fight bloody battles, such as Mosul (2016–2017), but due to principal-agent issues, SFA recipients are only as loyal to their SFA donor as their alignment of strategic interests. With SFA duties shifting from a SOF prerogative to conventional army duties, unconventional military operations have been mainstreamed.

Overall, the allure of SFA resides with the veneer of a cheap solution to leaders in Western capitals. They can demonstrate a willingness to deal with a security problem 'over there' and, at a minimum, provide minimal amounts of resources and military advisors to contain a security problem, without having to solve it. The grander problem lies with leaders in a weak state absorbing SFA and it being operationalised into long-term gains in security, stability, and economic development. In the rare case of SFA working, such as Colombia, success only occurred because political and military leadership had long-term horizons, and strategically absorbed security aid in a way that transformed the state and security institutions to address *Fuerzas Armadas Revolucionarias de Colombia* (FARC).[60]

The future dilemma for Western SFA providers is the balancing act. Determining how much SFA should be provided in relation to how much the state will absorb – and not creating dependencies. The other harsh reality for SFA providers is recipient state elites that are reluctant to create formalised institutions, fearing it might threaten their grip on personalised power. Regardless, SFA is a messy process that cannot be overcome through bureaucratised efficiency. Success in SFA is dependent upon influence, enduring partnerships, and convincing partners to make difficult reforms militarily and politically. At some point, with enough domestic political

willpower, the recipient state can strengthen institutions to create legitimacy, which can translate into the government being capable of providing safety and security in their own state.

Notes

1 Jahara Matisek and William Reno, 'Getting American Security Force Assistance Right: Political Context Matters', *Joint Force Quarterly* 92 (2019), 65–73.
2 Max Weber, *Max Weber on Law in Economy and Society*, M. Rheinstein and E. Shils, trans. (Cambridge, MA: Harvard University Press, 2006), 124–361.
3 Williamson A. Murray, 'The Industrialization of War 1815–1871', *The Cambridge History of Warfare*, G. Parker, ed. (New York: Cambridge University Press, 2005), 219–248; William H. Mott, *United States Military Assistance: An Empirical Perspective* (Westport, CT: Greenwood Publishing Group, 2002).
4 Roger E. Kanet, 'The Superpower Quest for Empire: The Cold War and Soviet Support for 'Wars of National Liberation'', *Cold War History* 6:3 (2006), 331–352.
5 Hew Strachan, ed., *Big Wars and Small Wars: The British Army and the Lessons of War in the 20th Century* (New York: Routledge, 2006); Martijn Kitzen, 'Western Military Culture and Counterinsurgency: An Ambiguous Reality', *Scientia Militaria: South African Journal of Military Studies* 40:1 (2012), 1–24.
6 David Armitage, *Civil Wars: A History in Ideas* (New Haven CT: Yale University Press, 2017), 50.
7 Jason Lyall, Isaiah Wilson, 'Rage against the Machines: Explaining Outcomes in Counterinsurgency Wars', *International Organization* 63:1 (2009), 67–106, Rupert A. Smith, *The Utility of Force: The Art of War in the Modern World* (London: Allen Lane, 2005), 6.
8 Keith B. Bickel, *Mars Learning: The Marine Corps' Development of Small Wars Doctrine, 1915–1940* (New York: Routledge, 2018).
9 James Barr, *Setting the Desert on Fire: TE Lawrence and Britain's Secret War in Arabia, 1916–1918* (New York: WW Norton & Company, 2008).
10 Mara E. Karlin, *Building Militaries in Fragile States: Challenges for the United States* (Philadelphia: University of Pennsylvania Press, 2018).
11 James A. Van Fleet, '25 Divisions for the Cost of One', *Readers Digest* 64 (1954), 85–98.
12 William Blum, *Killing Hope: US Military and CIA Interventions since World War II* (London: Zed Books, 2003).
13 Rob Johnson, *True to Their Salt: Indigenous Personnel in Western Armed Forces* (London: Oxford University Press, 2017), 293–335; Raymond F. Betts, *Decolonization* (New York: Routledge, 2004).
14 James D. Fearon, David D. Laitin, 'Ethnicity, Insurgency, and Civil War', *American Political Science Review* 97:1 (2003), 75–90.
15 Mary Kaldor, *New and Old Wars: Organised Violence in a Global Era* (Cambridge, UK: Polity Press, 2012).
16 Andreas Krieg, Jean-Marc Rickli, 'Surrogate Warfare: The Art of War in the 21st Century?', *Defence Studies* 18:2, 113–130.
17 Emily Knowles, Abigail Watson, *Remote Warfare: Lessons Learned from Contemporary Theatres* (London: Oxford Research Group, 2018), 1–2.
18 George W. Bush, *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2002), *European Security Strategy: A Secure Europe in a Better World* (Brussels: European Union, 2003).
19 Thomas R. Matelski, *Developing Security Force Assistance: Lessons from Foreign Internal Defense* (Fort Leavenworth KS: School of Advanced Military Studies,

2008), Robert L. Caslen Jr., *Afghan National Army (ANA): Mentor Guide* (Fort Leavenworth KS: JCISFA, 2011), vii.
20 Sydney J. Freedberg Jr., 'Guard Should Specialize in COIN: War College Study', *Breaking Defense*, 6 May 2016, https://breakingdefense.com/2016/05/guard-should-specialize-in-coin-war-college-study/.
21 'Army 2020 Refine', *British Army Website*, December 2016, https://web.archive.org/web/20171223032214/http://www.army.mod.uk/structure/33449.aspx.
22 Italian Army Colonel, PowerPoint Briefing, Rome, Italy, 24 September 2019.
23 Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973).
24 Ian Roxborough, 'Learning and Diffusing the Lessons of Counterinsurgency: The US Military from Vietnam to Iraq', *Sociological Focus* 39:4 (2006), 319–346.
25 Max Boot, 'The New American Way of War', *Foreign Affairs* 82:4 (2003), 41–58.
26 Stephen D. Biddle, 'Allies, Airpower, and Modern Warfare: The Afghan Model in Afghanistan and Iraq', *International Security* 30:3 (2006), 161–176.
27 Adam Scher, 'The Collapse of the Iraqi Army's Will to Fight: A Lack of Motivation, Training, or Force Generation?', *Army Press Online Journal* 16:8 (2016), 1–6; Colin D. Robinson, 'What Explains the Failure of US Army Reconstruction in Afghanistan?', *Defense & Security Analysis* 34:3 (2018), 249–266.
28 Jahara Matisek, 'The Crisis of American Military Assistance: Strategic Dithering and *Fabergé Egg* Armies', *Defense & Security Analysis* 34:3 (2018), 267–290.
29 Victor D. Hanson, *Carnage and Culture: Landmark Battles in the Rise to Western Power* (New York: Anchor, 2002).
30 Edward Ballanco, 'Security Force Assistance Needs the Stilwell Combination', *War Room*, 24 May 2019, https://warroom.armywarcollege.edu/articles/security-force-assistance-stilwell-combination/.
31 David H. Ucko, 'Systems Failure: The US way of Irregular Warfare', *Small Wars & Insurgencies* 30:1 (2019), 223–254.
32 Francesco Marone, *Oltre il concetto di Security Force Assistance: Nuove strategie ed efficacy soluzioni attuative per l'evoluzione delle attività di assistenza alle forze di sicurezza di una Host Nation* (Rome: Centro Militare Di Studi Strategici, 2017).
33 Barry R. Posen, 'Civil Wars & the Structure of World Power', *Dædalus* 146:4 (2017), 167–179.
34 Mark Langan, *Neo-Colonialism and the Poverty of 'Development' in Africa* (New York: Palgrave Macmillan, 2017), 149–175.
35 T.X. Hammes, 'Raising and Mentoring Security Forces in Afghanistan and Iraq', in *Lessons Encountered: Learning from the Long War*, R.D. Hooker Jr., J.J. Collins, eds. (Washington, DC: National Defense University Press, 2015), 332.
36 Ivor Wiltenburg and Martijn van der Vorm, 'Small State Strategic Thinking: The Case of the Netherlands', *The Strategy Bridge*, 23 September 2019, https://thestrategybridge.org/the-bridge/2019/9/23/small-state-strategic-thinking-the-case-of-the-netherlands.
37 'Resolute Support Mission (RSM): Key Facts and Figures', *NATO*, 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/20190625_2019-06-RSM-Placemat.pdf.
38 The White House, 'Fact Sheet: US Security Sector Assistance Policy', *Office of the Press Secretary*, 5 April 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy.
39 Robert M. Gates, 'A Balanced Strategy', *Foreign Affairs* 88:1 (2009), 28–40.
40 John L. Clarke, *What Roles and Missions for Europe's Military and Security Forces in the 21st Century* (Garmisch-Partenkirchen: George C. Marshall Center for Security Studies, 2005).
41 Judy Dempsey, 'Europeans Say No to Military Intervention', *Carnegie Europe*, 19 September 2013, https://carnegieeurope.eu/strategiceurope/53039.

42 Benjamin Haddad and Alina Polyakova, 'Is Going It Alone the Best Way Forward for Europe?', *Foreign Affairs*, 17 October 2018, https://www.foreignaffairs.com/articles/europe/2018-10-17/going-it-alone-best-way-forward-europe.
43 Knowles, Watson, *Remote Warfare: Lessons Learned*, 1–2.
44 Carnes Lord, 'American Strategic Culture in Small Wars', *Small Wars & Insurgencies* 3:3, (1992), 205–216; Robert M. Gates, 'Helping Others Defend Themselves: The Future of US Security Assistance', *Foreign Affairs* 89:3 (2010), 2–6.
45 Stephen Biddle, Julia Macdonald and Ryan Baker, 'Small Footprint, Small Payoff: The Military Effectiveness of Security Force Assistance', *Journal of Strategic Studies* 41:1–2 (2018): 89–142.
46 Jesse Dillon Savage and Jonathan D. Caverley, 'When Human Capital Threatens the Capitol: Foreign Aid in the Form of Military Training and Coups', *Journal of Peace Research* 54:4 (2017): 542–557; Richard A. Nielsen, 'Rewarding Human Rights? Selective Aid Sanctions against Repressive States', *International Studies Quarterly* 57:4 (2013), 791–803.
47 Maarten P. Broekhof, Martijn W.M. Kitzen, and Frans P.B. Osinga, 'A Tale of Two Mosuls, The resurrection of the Iraqi Armed Forces and the Military Defeat of ISIS', *Journal of Strategic Studies* 39:7 (2019), 1–23.
48 Elizabeth M. Bartels et al., *Conceptual Design for a Multiplayer Security Force Assistance Strategy Game* (Santa Monica, CA: RAND, 2019), 18.
49 William Reno, 'The Politics of Security Assistance in the Horn of Africa', *Defence Studies* 18:4 (2018), 498–513.
50 Lia Kent, Joanne Wallis, Srinjoy Bose, Miranda Forsyth, and Sinclair Dinnen, *Hybridity on the Ground in Peacebuilding and Development: Critical Conversations* (Acton, Australia: ANU Press, 2018).
51 Anders Themnér, ed., *Warlord Democrats in Africa: Ex-military Leaders and Electoral Politics* (London: Zed Books, 2017).
52 Karlin, *Building Militaries,* 2017.
53 *NATO SOF Military Assistance Handbook* (Mons, Belgium: NATO Special Operations Headquarters, 2014).
54 Ivor L. Wiltenburg, 'Security Force Assistance: Practised but not Substantiated', *Militare Spectator* 188:2 (2019), 88–99.
55 *Field Manual 31–20: Doctrine for Special Forces Operations* (Washington, DC: U.S. Department of Defense, 1990).
56 John F. Sopko, *Divided Responsibility: Lessons from U.S. Security Sector Assistance Efforts in Afghanistan* (Arlington, VA: SIGAR, 2019).
57 Interview, U.S. Army officer, 7 May 2020.
58 *The U.S. Army/Marine Corps Counterinsurgency Field Manual* (Chicago: University of Chicago Press, 2007).
59 Thomas Waldman, 'Vicarious Warfare: The Counterproductive Consequences of Modern American Military Practice', *Contemporary Security Policy* 39:2 (2018), 181–205.
60 Carlos G. Berrios, 'Critical Ingredient: US Aid to Counterinsurgency in Colombia', *Small Wars & Insurgencies* 28:3 (2017), 546–575.

References

Armitage, David, *Civil Wars: A History in Ideas* (New Haven, CT: Yale University Press, 2017).

Ballanco, Edward, 'Security Force Assistance needs the Stilwell Combination', *War Room*, 24 May 2019,
https://warroom.armywarcollege.edu/articles/security-force-assistance-stilwell-combination/

Bartels, Elizabeth M., et al., *Conceptual Design for a Multiplayer Security Force Assistance Strategy Game* (Santa Monica, CA: RAND, 2019).

Biddle, Stephen D., 'Allies, Airpower, and Modern Warfare: The Afghan Model in Afghanistan and Iraq', *International Security* 30:3 (2006), 161–176.

Biddle, Stephen, Macdonald, Julia, and Baker, Ryan, 'Small Footprint, Small Payoff: The Military Effectiveness of Security Force Assistance', *Journal of Strategic Studies* 41:1–2 (2018): 89–142.

Blum, William, *Killing Hope: US Military and CIA Interventions since World War II* (London: Zed Books, 2003).

Boot, Max, 'The New American Way of War'. *Foreign Affairs* 82:4 (2003), 41–58.

Broekhof, M.P., Kitzen, M.W.M., and Osinga, F.P.B., 'A Tale of Two Mosuls, The Resurrection of the Iraqi Armed Forces and the Military Defeat of ISIS', *Journal of Strategic Studies* 39:7 (2019), 1–23.

Bush, George W., *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2002).

Caslen Jr., Robert L., *Afghan National Army (ANA): Mentor Guide* (Fort Leavenworth, KS: JCISFA, 2011).

Clarke, John L., *What Roles and Missions for Europe's Military and Security Forces in the 21st Century* (Garmisch-Partenkirchen: George C. Marshall Center for Security Studies, 2005).

Dempsey, Judy, 'Europeans Say No to Military Intervention', *Carnegie Europe*, 19 September 2013, https://carnegieeurope.eu/strategiceurope/53039.

European Security Strategy: A Secure Europe in a Better World (Brussels: European Union, 2003).

Fearon, James D., and Laitin, David D., 'Ethnicity, Insurgency, and Civil War', *American Political Science Review* 97:1 (2003), 75–90.

Field Manual 31–20: Doctrine for Special Forces Operations (Washington, DC: U.S. Department of Defense, 1990).

Freedberg Jr., Sydney J., 'Guard Should Specialize in COIN: War College Study', *Breaking Defense*, 6 May 2016, https://breakingdefense.com/2016/05/guard-should-specialize-in-coin-war-college-study/

Gates, Robert M., 'A Balanced Strategy'. *Foreign Affairs* 88:1 (2009), 28–40.

Gates, Robert M., 'Helping Others Defend Themselves: The Future of US Security assistance', *Foreign Affairs* 89:3 (2010), 2–6.

Haddad, Benjamin, and Polyakova, Alina, 'Is Going It Alone the Best Way Forward for Europe?' *Foreign Affairs*, 17 October 2018, https://www.foreignaffairs.com/articles/europe/2018-10-17/going-it-alone-best-way-forward-europe.

Hammes, T.X., 'Raising and Mentoring Security Forces in Afghanistan and Iraq', in *Lessons Encountered: Learning from the Long War*, Richard D. Hooker, Joseph J. Collins, eds., 277–344 (Washington, DC: National Defense University Press, 2015).

Hanson, Victor D., *Carnage and Culture: Landmark Battles in the Rise to Western Power* (New York: Anchor, 2002).

Italian Army Colonel, PowerPoint Briefing. Rome, Italy. 24 September 2019.

Johnson, Rob, *True to Their Salt: Indigenous Personnel in Western Armed Forces* (London: Oxford University Press, 2017).

Kaldor, Mary, *New and Old Wars: Organised Violence in a Global Era* (Cambridge: Polity Press, 2012).

Kanet, Roger E., 'The Superpower Quest for Empire: The Cold War and Soviet Support for "wars of national liberation"', *Cold War History* 6:3 (2006), 331–352.

Karlin, Mara E., *Building Militaries in Fragile States: Challenges for the United States* (Philadelphia: University of Pennsylvania Press, 2018).

Kitzen, Martijn, 'Western Military Culture and Counterinsurgency: An Ambiguous Reality', *Scientia Militaria: South African Journal of Military Studies* 40:1 (2012), 1–24.

Knowles, Emily, and Matisek, Jahara, 'Western Security Force Assistance in Weak States: Time for a Peacebuilding Approach', *The RUSI Journal* 164:3 (2019), 10–21.

Knowles, Emily, and Watson, Abigail, *Remote Warfare: Lessons Learned from Contemporary Theatres* (London: Oxford Research Group, 2018).

Krieg, Andreas, and Rickli, Jean-Marc, 'Surrogate Warfare: The Art of War in the 21st Century?', *Defence Studies* 18:2, 113–130.

Langan, Mark, *Neo-Colonialism and the Poverty of 'Development' in Africa* (New York: Palgrave Macmillan, 2017).

Lord, Carnes, 'American Strategic Culture in Small Wars', *Small Wars & Insurgencies* 3:3, (1992), 205–216.

Lyall, Jason, and Wilson, Isaiah, 'Rage against the Machines: Explaining Outcomes in Counterinsurgency Wars'. *International Organization* 63:1 (2009), 67–106.

Marone, Francesco, *Oltre il concetto di Security Force Assistance: Nuove strategie ed efficacy soluzioni attuative per l'evoluzione delle attività di assistenza alle forze di sicurezza di una Host Nation* (Rome: Centro Militare Di Studi Strategici, 2017).

Matelski, Thomas R., *Developing Security Force Assistance: Lessons from Foreign Internal Defense* (Fort Leavenworth, KS: School of Advanced Military Studies, 2008).

Matisek, Jahara, 'The Crisis of American Military Assistance: Strategic Dithering and Fabergé Egg Armies', *Defense & Security Analysis* 34:3 (2018), 267–290.

Matisek, Jahara, and Reno, William, 'Getting American Security Force Assistance Right: Political Context Matters', *Joint Force Quarterly* 92 (2019), 65–73.

Mott, William H., *United States Military Assistance: An Empirical Perspective* (Westport, CT: Greenwood Publishing Group, 2002).

Murray, Williamson A., 'The Industrialization of War 1815–1871', in *The Cambridge History of Warfare*, Geoffrey Parker, ed., 219–248 (New York: Cambridge University Press, 2005).

NATO, 'Resolute Support Mission (RSM): Key Facts and Figures'. *NATO*, 2019,
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/20190625_2019-06-RSM-Placemat.pdf.

NATO SOF Military Assistance Handbook (Mons, Belgium: NATO Special Operations Headquarters, 2014).

Nielsen, Richard A., 'Rewarding Human Rights? Selective Aid Sanctions against Repressive States', *International Studies Quarterly* 57:4 (2013), 791–803.

Posen, Barry R., 'Civil Wars & the Structure of World Power', *Dædalus* 146:4 (2017), 167–179.

Reno, William, 'The Politics of Security Assistance in the Horn of Africa', *Defence Studies* 18:4 (2018), 498–513.

Robinson, Colin D., 'What Explains the Failure of US Army Reconstruction in Afghanistan?' *Defense & Security Analysis* 34:3 (2018), 249–266.

Roxborough, Ian, 'Learning and Diffusing the Lessons of Counterinsurgency: The US military from Vietnam to Iraq', *Sociological Focus* 39:4 (2006), 319–346.

Savage, Jesse Dillon, and Caverley, Jonathan D., 'When Human Capital Threatens the Capitol: Foreign Aid in the Form of Military Training and Coups', *Journal of Peace Research* 54:4 (2017): 542–557.

Scher, Adam, 'The Collapse of the Iraqi Army's Will to Fight: A Lack of Motivation, Training, or Force Generation?' *Army Press Online Journal* 16:8 (2016), 1–6.

Sepp, Kalev I., 'Best Practices in Counterinsurgency', *Military Review* (May–June 2005), 8–12.

Smith, Rupert A., *The Utility of Force: The Art of War in the Modern World* (London: Allen Lane, 2005).

Sopko, John F., *Divided Responsibility: Lessons from U.S. Security Sector Assistance Efforts in Afghanistan* (Arlington, VA: SIGAR, 2019).

Strachan, Hew, ed., *Big Wars and Small Wars: The British Army and the Lessons of War in the 20th Century* (New York: Routledge, 2006).

The U.S. Army/Marine Corps Counterinsurgency Field Manual (Chicago: University of Chicago Press, 2007).

The White House, 'Fact Sheet: US Security Sector Assistance Policy', *Office of the Press Secretary*, 5 April 2013,
https://obamawhitehouse.archives.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy.

Ucko, David H., 'Systems Failure: The US Way of Irregular Warfare', *Small Wars & Insurgencies* 30:1 (2019), 223–254.

Van Fleet, James A., '25 Divisions for the Cost of One', *Readers Digest* 64 (1954), 85–98.

Waldman, Thomas, 'Vicarious Warfare: The Counterproductive Consequences of Modern American Military Practice', *Contemporary Security Policy* 39:2 (2018), 181–205.

Weber, Max, *Max Weber on Law in Economy and Society*, Max Rheinstein and Edward Shils, trans. (Cambridge, MA: Harvard University Press, 2006).

Weigley, Russell F., *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973).

Wiltenburg, Ivor L., 'Security Force Assistance: Practised but not Substantiated', *Militare Spectator* 188:2 (2019), 88–99.

Wiltenburg, Ivor, and Van der Vorm, Martijn, 'Small State Strategic Thinking: The Case of the Netherlands', *The Strategy Bridge*, 23 September 2019, https://thestrategybridge.org/the-bridge/2019/9/23/small-state-strategic-thinking-the-case-of-the-netherlands.

12 Learning and forgetting counterinsurgency

Martijn van der Vorm

Introduction

In 2011 an air campaign by Western militaries helped in disposing the regime of Muammar Gaddafi in Libya. Ostensibly learning from their experiences in Iraq and Afghanistan not to become embroiled in messy state building campaigns, the intervening powers largely disengaged militarily from Libya. Despite this application of hard earned wisdom, a civil war ensued over the spoils of Libya with serious repercussions for the wider region. Yet again in the 21st century, a Western military intervention yielded adverse strategic effects.[1] While this example primarily shows a lack of understanding about the utility of military at the political level, the air campaign over Libya also challenges the ability of the armed forces to retain the knowledge from recent operations. Ironically, academic publications on how armed forces learn during conflict have proliferated tremendously over the last 20 years.[2] This can be largely ascribed to Western militaries' experiences during the large-scale counterinsurgency efforts in Iraq and Afghanistan.[3] Initially, the militaries involved were unprepared – conceptually as well as practically – to conduct counterinsurgency operations.[4] Prior knowledge on how to conduct counterinsurgency had been forgotten, misremembered or discarded. Arguably, the most well-known example in this regard is the U.S. failure to preserve hard-gained knowledge from Vietnam. In this case the armed forces apparently seemed to purge themselves of the counterinsurgency experiences from that unsuccessful war.[5] In the United Kingdom, a similar pattern of strategic amnesia could be observed as the rich experiences of the past were seemingly forgotten by the advent of the 21st century.[6] This dynamic of forgetting knowledge from previous experiences meant that Western militaries have to (re)learn how to conduct counterinsurgency operations.

Now that large-scale counterinsurgency campaigns have ended, the interest in the concept of counterinsurgency is, again, in decline. Indeed, the disenchantment with counterinsurgency missions and the broader concept in the West is notable as was apparent in the case of Libya.[7] This weariness has led several scholars and officers to argue that Western armed forces are in

the process of forgetting the hard-won lessons from Iraq and Afghanistan.[8] This would mean a new turn of the recurring cycle of learning, forgetting and relearning counterinsurgency knowledge.

If Western militaries have proven to be adept at learning during recent unsuccessful counterinsurgency campaigns, but discard this knowledge afterwards, this apparent aptitude is nothing more than a consolation prize. This chapter, therefore, hypothesises that the lessons learned from a conflict are perceived and handled differently after the conflict has ended, with a potentially altered strategic environment, then during the conflict itself. While this chapter focuses on learning from counterinsurgency operations, the question of how knowledge is retained after conflict is of course germane for any type of conflict.

The objective of this chapter is to examine the processes of how armed forces learn from irregular conflict. To this end, the chapter is divided into four sections. The first section explores the literature on how militaries learn and change in relation to conflict. The second section examines the process of informal learning in conflict. In the third section the dynamics of more formal organisational learning are explored. The fourth and final section analyses the dynamics of knowledge retention in a new strategic environment. This chapter concludes with an assessment of why transferring knowledge from recent counterinsurgency experiences continues to be difficult in Western armed forces and why this subject provides ample opportunity for additional research.

Learning from conflict

The ability to adapt and learn in war is regarded essential to overcome surprise on the battlefield.[9] As war is considered a competition of wills, adversaries of any stripes will seek to adapt in order to gain an advantage in conflict either through committing additional resources, implementing new technologies, trying new concepts or a combination of those elements.[10] Evidently, this holds true for all belligerents in war. If one side cannot adapt to the challenges posed by combat and the environment, staving off defeat will become very hard.[11] This is not to say that proficiency in learning is a guarantee for success.[12]

The academic subfield of 'military innovation studies' examines how armed forces enact organisational change. It encompasses change in military organisations through the adoption of novel technologies and concepts, reorganisations that are forced on the armed forces by their political or military leadership and drawing lessons from conflicts.[13] As such, military innovation studies cannot be regarded solely as a specific and applied element of organisational learning literature. Thus far the diverse manifestations of change in military organisations have precluded the establishment of an overarching theory that explains such change. As a result, military innovation studies have drawn critique for lack of theoretical clarity.[14]

This critique notwithstanding, the subfield of military innovation studies has distinct redeeming qualities. First of all, it has yielded a wealth of empirical case studies on learning by military organisations. Although a significant portion of these works describe the recent counterinsurgency campaigns in Iraq and Afghanistan, other historical conflicts have also been studied extensively. Second, military innovation studies have classified the various manifestations of change in military organisations that can be the result of learning processes. These manifestations of change include doctrine, organisational structures, military strategy, operations and education and training.[15] A third and most salient contribution is the identification of many factors of influence that shape learning processes. Internal factors are organisational culture, leadership and internal learning, and dissemination arrangements. In principle, however, such internal factors are not unique to military organisations.[16] External factors such as domestic politics, alliance politics, civil-military relations, strategic culture, defence policy and resources are more specific to the context of military organisations.[17] Finally, scholars studying military change have increasingly applied organisational learning theory to their research. Most of this research is concerned with how armed forces learn during conflict.[18] In this body of literature, a distinction is made between informal learning that is initiated in, and shared between, deployed units, and adaptations that are facilitated by the wider organisation. The latter iteration corresponds with the notion that lessons must be accepted by the organisations' leadership in order to be implemented and disseminated throughout the entire organisation. How lessons are retained after conflict is also a subject of study. In most of this research, the manifestation of learning from previous wars is focused on doctrine.[19] For a more comprehensive understanding of the military organisational learning process in relation to war, the acquisition, implementation and dissemination of knowledge in conflict should be studied, as well as the subsequent retention of knowledge after the conflict has ended.

Informal learning in conflict

After the short conventional campaigns that toppled the incumbent regimes in Afghanistan and Iraq, Western armed forces were caught flat-footed when full-fledged insurgencies erupted.[20] Due to the institutional neglect of counterinsurgency knowledge in Western militaries, the understanding needed to operate in such complex environments had been lost. By and large, units in the field were struggling to understand the operational environment, confront their elusive adversaries and stem the violence.

Invariably, tactical units seek to overcome such challenges on their own initiative. This starts with identifying deficiencies in their current performance. Examples of indicators of deficiencies can be amongst other things, increasing levels of violence in the area of operations, or mounting casualties inflicted by Improvised Explosive Devices (IEDs).[21] From the

perspective of the troops, these incentives to learn are compelling. Because of the immediate impact of these deficiencies and the high operational pace, units cannot wait for organisational solutions.[22] Moreover, due to the typically dispersed nature of operations, local units have the best knowledge of the operational environment. Thus, deployed units and their commanders must be empowered to experiment with battlefield solutions to overcome tactical problems.

To address deficiencies, troops can experiment with tactics, techniques and procedures, adjust their organisation and improvise equipment. During operations, these measures can be tested, evaluated and adjusted. Units in the field routinely evaluate their operations, both to recognise shortfalls and to share best practices within the unit or with adjacent units. This ensures that the cycle of learning and adapting is continuous and dynamic. Ideally, this acquired knowledge is horizontally shared with other units simultaneously in theatre or to subsequent rotations who might encounter similar challenges. This dynamic can occur through informal instruction or publications.[23] For example, the first Dutch special forces detachment in Uruzgan in 2006 shared their best practices with the incoming Dutch Battle Group during an informal session. In turn, the special forces had learned most of these lessons from their Australian and American counterparts.[24]

In this regard, the notion of informal learning does not mean that organisational arrangements are irrelevant. When the military organisation allows individuals, such as unit commanders, sufficient latitude to improvise and adapt, this can instil a culture in which innovative ideas can thrive.[25] As a unit cannot draw on additional resources in informal learning, the assets available to the commander shape the range of solutions available to him. A divisional commander like David Petraeus in Mosul in 2003 could draw from extensive resources under his command to pursue a population-centric counterinsurgency strategy rather than conventional clearing operations. By restraining the use of force, emphasising intelligence collection and providing basic services to the population, this approach succeeded in decreasing the levels of violence in the area.[26] Other organisational arrangements such as the Commander's Emergency Response Program (CERP), that could be employed at the commander's discretion, further increase resources that could be used to act on lessons learned during operations.[27]

An example of informal learning in a smaller unit is that of a U.S. marine battalion in Iraq in 2006 that reinforced its intelligence section from four officers to over 30 analysts to keep abreast of the vast amount of information coming from the field.[28] This decision was entirely within the purview of the battalion commander. Yet, he will not have taken this decision lightly as this additional intelligence personnel had to come from within the battalion and therefore could not perform their organic tasks such as conducting patrols.[29] While this approach yielded results, it did not lead to augmented intelligence sections within all Marine and Army battalions or brigades.

Beyond organisational culture, leadership that is willing to experiment is a crucial factor of influence in informal learning.

Evidently, there are inherent limits to informal learning in conflict. A key constraint of informal learning is that the scope of learning is innately limited to the resources a unit has to its disposal. Another constraint is that without institutional attention towards the learning process, the organisation cannot ensure that the lessons learned are coherent with each other and the organisation's strategy. Finally, the dissemination of knowledge depends on informal networks. This means that when the experience from past campaigns is not formally incorporated and shared, the acquired knowledge can prove ephemeral.[30]

Organisational adaptation in conflict

If an armed force as a whole acknowledges deficiencies and accepts proposed solutions, these can be disseminated and implemented in a more coherent and systemic fashion. Implemented adaptations pertain to the theatre of operations and the organisational structures that support the mission. However, the organisational response can be sluggish.

A telling example of the institutional reluctance to act on requests from the field is the glacial process by the U.S. Marine Corps to acquire Mine-Resistant Ambush-Protected Vehicles (MRAPs). When deployed Marine units recognised that the threat of IEDs had grown beyond their own ability to mitigate this challenge through altered procedures, MRAPs were identified as a solution to provide mobility with adequate protection. While the need for MRAPs was identified early on, the procurement was delayed at the institutional level because it would endanger other materiel acquisitions that the U.S. Marine Corps prioritised. In the end, it took two years before the MRAPs were deployed to Iraq.[31] Other examples of slow organisational adaptation during conflict include training exercises before deployment. American units continued to train for conventional operations in preparation to their mission in Iraq in 2004.[32] Furthermore, an American in-theatre counterinsurgency school for Iraq was only established in 2005.[33]

Thus, the formal integration of knowledge from the field is typically a lengthy process. First of all, the institution must share the analysis that the identified deficiencies warrant its attention.[34] Second, organisational structures must be in place to collect, analyse and distribute knowledge from the field.[35] Third, the organisation and the units in theatre can differ in opinion about the best solution for the identified challenges as the example of the procurement of MRAPs shows. Moreover, the allocation of additional budget or manpower to theatre often requires political approval.[36] As a result, political considerations can influence (and hinder) the implementation of lessons learned.

The primary example of recent organisational learning in conflict is the publication in 2006 of the American *Field Manual* on counterinsurgency

(*FM 3-24*) and the subsequent change in strategy for Iraq. As the situation in Iraq deteriorated, the U.S. Army and Marine Corps were driven to review their approach to the war. In other words, the institution as a whole recognised the deficiency in its performance relative to its environment and was open to utilise new knowledge for remedial action.[37] Organisational mechanisms for knowledge acquisition and dissemination, in the form of the U.S. Army's Combined Arms Center (CAC), shifted into high gear to search for solutions to this problem.[38] The main product of this effort was the *FM 3-24* which offered guidance on the conduct of population-centric counterinsurgency operations. American forces would strive to protect the population and assist in providing basic services instead of focusing solely on targeting elusive insurgents. This doctrinal document was in large part inspired by the informal lessons learned by deployed units.[39] The formalisation of these lessons and the publication of an official field manual were crucial steps in organisational learning during conflict. However, these efforts were by no means a guarantee that these lessons would be implemented, especially as there was extensive critique on the counterinsurgency doctrine and its proponents.[40]

Only when President Bush decided in early 2007 to try salvage the American mission in Iraq, the U.S. military could put the lessons into practice. Concurrently, Bush endorsed the implementation of a population-centric approach as envisioned by *FM 3-24*. The sponsor of the doctrine, Petraeus, was to oversee its application as commander in Iraq. Critically, Bush signed off on additional troops that were needed to make this strategy work. Whether or not this 'Surge' was responsible for the subsequent decrease in violence in Iraq, it is a seminal example of organisational learning in war. The lessons were manifested in new doctrine, strategy, tactics, force preparation and increased troop levels. In addition, this example shows the manifold factors influencing the process: domestic politics, civil-military relations, leadership, available resources, organisational culture, internal politics and institutional arrangements for knowledge production and distribution. All these factors were aligned sufficiently to facilitate the U.S. military's adaptation to counterinsurgency.

Yet, despite profound efforts from Western armed forces to learn from their experiences in Iraq and Afghanistan, the formal organisational learning processes have been constrained as well. First of all, just like some units and their commanders did not adapt informally to operational challenges, others ignored the knowledge and lessons that were disseminated by the institutions. Commanders in Iraq and Afghanistan defaulted to more conventional approaches, as they felt that population-centric counterinsurgency was incompatible with their units' regular task and training.[41] A second limitation typical to organisational learning in irregular conflict is the endurance of lessons beyond the last conflict. When the strategic context has changed, the hard-won lessons of the previous war are often viewed in a different perspective. The next section will elaborate on the current focusing

by Western militaries on great power competition and conventional warfare. Armed forces that only reluctantly adapted to challenges of counterinsurgency campaigns can then revert back to their traditional outlook, thereby discarding the knowledge from past conflicts.

Knowledge retention after conflict

A crucial factor influencing the retention of lessons from previous conflicts is how the contemporary strategic environment is assessed. The success of incorporating lessons and enact other changes in military organisations depends in a large part to the extent these are congruent with political guidance and the threat perception.[42] Indeed, with the end of the large-scale commitments in Iraq and Afghanistan, the strategic outlook of most Western states has changed dramatically. Strategic challenges such as countering the Russian Federation, China, Iran and the Islamic State's aspirations have garnered the attention of Western policy makers. As a result, Western militaries are in the process of recalibrating towards fighting high-intensity conventional wars.[43] According to some observers, the previous emphasis on counterinsurgency missions has led to an erosion of Western combat capabilities.[44] In this light, armed forces are reluctant to institutionalise lessons from counterinsurgency campaigns and other missions than conventional combat. Without the operational pressures of massive deployments in such missions, militaries will prioritise preparation for conventional warfare as this is (perceived) to be their core task.[45]

Concurrently, Western militaries continue to be deployed to intrastate conflicts, albeit in a more limited and indirect role. Current commitments are largely fulfilled by Special Operations Forces (SOF) or through Security Force Assistance (SFA) missions (for an extensive explanation of SFA, see the previous chapter by Matisek and Wiltenburg).[46] Moreover, the main strategic incentive for many U.S. allies to participate in the war in Afghanistan was in the first place to be a 'good ally'.[47] Retention of military lessons was therefore not a primary concern after this conflict. In this context, however, the more practical risk of evaporation of counterinsurgency knowledge is palpable. Institutional resources and attention are diverted to other mission types. If this knowledge is not institutionalised, all the formal and informal adaptations in Iraq and Afghanistan will be lost to posterity. Given the continuous involvement of Western militaries in intrastate conflict, this is highly undesirable as the experience of previous counterinsurgency campaigns will hold relevant lessons for future missions.[48]

Institutionalisation of prior experience is not a normative prescription, in the sense that this is always beneficial to a military organisation. Learning the wrong lessons from the past can be as detrimental to armed forces as not learning at all.[49] The applicability of lessons learned must therefore be analysed within the new strategic context and towards potential future threats. Future intrastate conflicts will be different from either the wars in Iraq and

Afghanistan. Indeed, these two conflicts had very dissimilar characteristics and lessons from the one could not be implemented blindly to the other.[50] However, these recent conflicts should not be regarded as aberrations that have no bearing on future wars.[51] After all, due to the neglect of counterinsurgency knowledge before the wars in Iraq and Afghanistan, troops had to relearn these lessons under fire.

An important step for retaining knowledge is internal mission evaluations. By examining the conduct of operations, deficiencies and lessons may be identified. For instance, the U.S. Army has published a thorough, unclassified evaluation of its performance during the war in Iraq, while the British army conducted a classified study of its campaign in Afghanistan.[52] This document candidly analyses mistakes by commanders in the preparation of the war, the subsequent occupation and countering a multifaceted insurgency. Such internal scrutiny is essential to identify what worked in the context of a conflict and helps preventing historical myth building.

Thus, to ensure that relevant knowledge is available for future conflicts, it must be consciously stored within the organisational memory. While writing evaluations and doctrine are essential steps in analysing the relevance of lessons, they are insufficient for real institutionalisation. Instead, the lessons should be reflected in the curricula of military academies and command and staff colleges. Furthermore, available knowledge should inspire training scenarios so military personnel can get acquainted with it in controlled environments.[53] For instance, the 1 (German/Netherlands) Corps has sought to integrate the 'comprehensive approach' into its exercise schedule based on its experiences in Afghanistan. Every year, an exercise by the name 'Common Effort' is held, in which interagency partners, international organisations and non-governmental organisations participate. The objective of this exercise is to ensure understanding and knowledge sharing among civilian organisations and armed forces who are invariably confronted with the same security challenges. By training together regularly, these organisations should be able to cooperate better in future conflicts.[54]

Other manifestations of institutionalisation can be the procurement of new material or the establishment of new organisational structures. An example of the former is the procurement by the Royal Netherlands Air Force of Unmanned Aerial Vehicles (UAVs) of the MQ-9 (Reaper), based on lessons from the Dutch mission in Afghanistan. This acquisition was however repeatedly delayed by lack of budget, despite the operational need of these UAVs. This acquisition also led to the establishment of new organisational elements such as the squadron for the UAVs, as well as a unit that will process and analyse the data collected by the unmanned platforms.[55] Another example of new organisational structures based on recent experiences is the establishment of the U.S. Army's new Security Force Assistance Brigades (SFABs). The purpose of these brigades is to 'develop the capacity and capability of foreign security forces to facilitate the achievement of US strategic objectives, in coordination with joint, interagency, and multinational

forces'. Based on its experiences in Iraq and Afghanistan, the U.S. Army has recognised a deficiency in its performance in training and mentoring local forces. The new SFABs are meant to address this deficiency, in part by specifically selecting and training personnel for conducting SFA missions.[56]

Cases like these show that some lessons from the recent counterinsurgency campaigns have indeed been acknowledged for use in future conflict. Whether such examples are isolated specks of institutionalisation or an indication that knowledge retention from counterinsurgency campaigns is indeed actively pursued by (some) Western militaries is subject to further research. Most academic observers are sceptical on this matter.[57] Beyond the uncertainty of the contemporary strategic environment, other factors can have profound influence on the ability to maintain or implement acquired lessons. Most fundamental, perhaps, is the question of what resources are available to the armed forces. If budgets are tight, organisational structures tasked with knowledge retention and dissemination are often axed in favour of operational needs.[58] In addition, when the organisation promotes conventional career paths over specialisations such as counterinsurgency or SFA, such competencies are vulnerable to wither as military personnel will perceive these specialisations as detrimental to their careers.[59] The interplay of such organisational and environmental factors makes studying learning after conflict complex, perhaps even more so than learning during conflict. Arguably, this complexity can make studying this strand of learning the most interesting. At the very least however, it must be included in the research on how armed forces learn in relation to conflict.

Conclusion

As the vast body of literature attests, Western armed forces have strived to cope with the operational challenges posed by the counterinsurgency campaigns of the early 21st century. Deployed troops and the wider organisations have tried to use their experiences to enact changes within their doctrines, concepts, procedures, equipment, education and organisational structures to enhance their performance during conflict. Although improvements on the tactical and operational levels of the campaigns have not yielded strategic successes, the ability to learn and adapt has been profound on many occasions. Yet, successful instances of informal and organisational adaptation must not eclipse the retention of these lessons when the conflict has ended. Rather, learning should be regarded as a continuous process that is not truncated by specific conflicts.

This chapter has distinguished between three strands of military learning in relation to conflict. First of all, there is the informal learning by deployed units that seeks to address immediate deficiencies during operations. Second, a more formal strand of learning exists in which the wider organisation provides resources and attention to the learning process within a given conflict. This process can be initiated by the organisational leadership, but

can also originate from informal lessons. The third strand is that of learning from the previous conflict. When the strategic environment has changed how is the relevance of knowledge from the last war assessed? How can military organisations ensure that this knowledge is available for future conflicts?

While the strands of informal and formal learning during recent counterinsurgency operations have been studied extensively, the third strand of preserving hard-won knowledge for future conflicts also warrants institutional and academic attention. This research can offer answers to pertinent questions. For instance, what lessons have been institutionalised by Western armed forces and why? What factors influencing the process of learning have the most impact and how do they interact? Are there variations observable between Western states on what lessons they derive from seemingly similar experiences? A final subject for research can be how knowledge retention works in relation to other types of conflict.

Beyond academic relevance, the different strands of learning have a significant bearing on the actual conduct of contemporary warfare. To be sure, deployed units have to show the ability to adapt within any conflict. However, irregular adversaries increasingly have access to knowledge and new technologies. Often, they do not have to overcome organisational barriers to implement new capabilities. Therefore, informal learning must be fostered in Western militaries to expedite their learning cycle in war, for instance by investing in educating personnel to assess the environment, providing leeway to experiment and perhaps even discretionary funds to implement adaptations. Potentially, if the informal learning processes become more empowered, formal learning during conflict could be more focused on the campaign and strategic levels to ensure coherence in the tactical activities towards the strategic objectives. In recent wars, most manifestations of formal learning were centred on acquisition of equipment and disseminating best practices. While the example of the American overhaul of the Iraq campaign in 2006–2007 is germane, it was indeed an exceptional manifestation of formal learning.

Finally, the institutionalisation of knowledge after conflict is important in order to retain it. This requires more than writing it down in arcane tomes of doctrine that are hardly read. In addition, the knowledge should be reflected in education, training and organisational structures. To implement relevant lessons, military organisations must be willing to ask hard questions about their prior performance and challenge institutional norms. Given the propensity of Western states to intervene in intrastate irregular wars, relevant knowledge from recent experience must be available for future conflicts. While learning and adapting is crucial in any war, we must ensure that we have a foundation to build from, based on our extensive experiences in counterinsurgency campaigns. Purging our military institutions of these experiences in irregular warfare ensures that these lessons eventually have to be relearned during operations in future conflicts. Consequently, it will be the deployed service members and the local population that will bear the costs of this recurring strategic amnesia.

Notes

1 Frank Ledwidge, *Losing Small Wars* (New Haven, CT: Yale University Press, 2017),109–112.
2 James Russell, *Innovation, Transformation and War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005–2007* (Stanford, CA: Stanford University Press, 2011); Chad Serena, *A Revolution in Military Adaptation: The US Army in Iraq* (Washington, DC: Georgetown University Press, 2011).
3 See for example, Stuart Griffin, 'Military Innovation Studies: Multidisciplinary or Lacking Discipline', *The Journal of Strategic Studies* 40:1–2 (2017), 196–224; Tom Dyson, 'The Military as Learning Organisation: Establishing the Fundamentals of Best-practice in Lessons Learned', *Defence Studies* 19:2 (2019), 107–129.
4 David Ucko, *The New Counterinsurgency Era* (Washington, DC: Georgetown, 2009), 9–12.
5 Richard Downie, *Learning from Conflict: The U.S. Military in Vietnam, El Salvador, and the Drug War* (Westport, CT: Praeger, 1998), 110–122.
6 Ledwidge, *Losing Small Wars*, 146–166.
7 Beatrice Heuser and Eitan Shamir, 'Universal Toolbox, National Styles or Divergence of Civilisations?', in *Insurgencies and Counterinsurgencies: National Styles and Strategic Cultures*, B. Heuser, E. Shamir, eds. (New York: Cambridge University Press, 2016), 367.
8 Jason Clark, ''Good Allies': International Perspectives on Afghanistan', *The War Room*, 29 March 2019.
9 Meir Finkel, *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield* (Stanford, CA: Stanford University Press, 2011), 223–226.
10 Lawrence Freedman, *The Future of War: A History* (London: Penguin, 2017), 277–279.
11 Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Delft: Eburon Academic Publishers, 2005), 273–274, Eliot Cohen, John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Free Press, 2006), 26–28.
12 Aimee Fox, *Learning to Fight: Military Innovation and Change in the British Army, 1914–1918* (Cambridge: Cambridge University Press, 2018), 9.
13 Rob Sinterniklaas, *Military Innovation: Cutting the Gordian Knot* (Breda: Netherlands Defence Academy, 2018), 5–11.
14 Adam Grissom, 'The Future of Military Innovation Studies', *The Journal of Strategic Studies* 29:5 (2006), 905–934, Griffin, 'Military Innovation Studies', 196–201.
15 Sinterniklaas, *Military Innovation*, 31.
16 Frank Hoffman. *Learning While Under Fire: Military Change in Wartime* (London: King's College, 2015), 233–240.
17 Theo Farrell, 'Introduction: Military Adaptation in War', in *Military Adaptation in Afghanistan*, T. Farrell, F. Osinga, J. Russell, eds. (Stanford, CA: Stanford University Press, 2013), 12.
18 Nina Kollars, 'Organising Adaptation in War', *Survival* 57:6 (2015): 111–126, Sergio Catignani, 'Coping with Knowledge: Organizational Learning in the British Army?', *The Journal of Strategic Studies* 37:1 (2014), 30–64.
19 Benjamin Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford, CA: Stanford University Press, 2016), David Fitzgerald, *Learning to Forget: US Army Counterinsurgency Doctrine and Practice from Vietnam to Iraq* (Stanford, CA: Stanford University Press, 2013).
20 Jeremy Black, *Insurgency and Counterinsurgency: A Global History* (Lanham, MD: Rowman & Littlefield, 2016), 206–210.

21 Serena, *A Revolution in Military Adaptation,* 107–108.
22 Nina Kollars, 'Military Innovation's Dialectic: Gun Trucks and Rapid Acquisition', *Security Studies* 23:4 (2014), 787–788.
23 Robert Foley, 'Dumb Donkeys or Cunning Foxes? Learning in the British and German Armies during the Great War', *International Affairs* 90:2 (2014), 279–298, Nina Kollars, 'War's Horizon: Soldier-Led Adaptation in Iraq and Vietnam', *The Journal of Strategic Studies* 38:4 (2015), 529–553.
24 George Dimitriu, Gijs Tuinman, and Martijn van der Vorm, 'Formative Years: Military Adaptation of Dutch Special Operations Forces in Afghanistan', *Special Operations Journal* 2:2, 156–157.
25 Russell, *Innovation, Transformation and War*, 70–71.
26 Mark Moyar, *A Question of Command: Counterinsurgency from the Civil War to Iraq* (New Haven, CT: Yale University Press, 2009), 220–226.
27 Eli Berman, Joseph Felter, and Jacob Shapiro, *Small Wars, Big Data: The Information Revolution in Modern Conflict* (Princeton, NJ: Princeton University Press, 2018), 123–128.
28 James Russell, *Innovation, Transformation and War*, 69.
29 Ibid.
30 Sjoerd de Winter, *The Army after Afghanistan: A Case Study on Military Adaptation to Counterinsurgency Warfare within 12 Infantry Battalion Air Assault the Regiment Van Heutsz* (Breda: Netherlands Defence Academy, 2015), 47–49.
31 Frank Hoffman, *Learning While Under Fire*, 212–214.
32 John Nagl, *Knife Fights: A Memoir of Modern War in Theory and Practice* (New York: Penguin, 2014), 64–70.
33 Brian Burton and John Nagl, 'Learning as We Go: The US Army Adapts to Counterinsurgency in Iraq, July 2004–December 2006', *Small Wars & Insurgencies* 19:3 (2008), 318–319.
34 Downie, *Learning from Conflict,* 24, Andrew Hill and Stephen Gerras, 'Systems of Denial', *Naval War College Review* 69:1 (2016), 113.
35 Serena, *A Revolution in Military Adaptation,* 111–119.
36 Farrell, 'Introduction', 12.
37 Hill, Gerras, 'Systems of Denial', 109–132.
38 Conrad Crane, *Cassandra in Oz* (Annapolis: Naval Institute Press, 2016), 41–46.
39 Ucko, *The New Counterinsurgency Era*, 108.
40 Gian Gentile, 'A (Slightly) Better War: A Narrative and Its Defects', *World Affairs* 171:1 (2008), 57–64, Douglas Porch, 'The Dangerous Myths and Dubious Promise of COIN', *Small Wars & Insurgencies* 22: 2 (2011), 239–257 .
41 Sergio Catignani, "Getting COIN' at the Tactical Level in Afghanistan: Reassessing Counter-Insurgency Adaptation in the British Army', *Journal of Strategic Studies* 35:4 (2012), 521–523.
42 Williamson Murray, 'Innovation: Past and Future', in *Military Innovation in the Interwar Period*, W. Murray and A. Millet, eds. (New York: Cambridge University Press, 1996), 304–306.
43 United States Department of Defense, *National Defense Strategy 2018* (Washington, DC: U.S. Department of Defense, 2018); HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* (London, 2015).
44 Douglas Porch, *Counterinsurgency: Exposing the Myths of the New Way of War* (New York: Cambridge University Press, 2013), 318–345; Otto van Wiggen, Robbert-Jan Aarten, 'Oefening Bison Drawsko 2017: Een essentiële nulmeting voor de Landmacht', *Militaire Spectator* 186:12 (2017), 581–596.
45 Hans Hasselbladh, Karl Yden, 'Why Military Organizations Are Cautious About Learning?', *Armed Forces & Society* (2019), 15–17.

46 Thomas Waldman, 'Vicarious Warfare: The Counterproductive Consequences of Modern American Military Practice', *Contemporary Security Policy* 39:2 (2018), 198–199.
47 Clarke, 'Good Allies'.
48 Berman, Felter, and Shapiro, *Small Wars, Big Data,* 8–12.
49 Eric Sangar, 'The Pitfalls of Learning from Historical Experience: The British Army's Debate on Useful Lessons for the War in Afghanistan', *Contemporary Security Policy* 37:2 (2016), 223–245.
50 Bryan Riddle, *Essence of Desperation* (Lanham, MD: Lexington Books, 2018), 103–110.
51 William Fuller, 'What Is a Military Lesson?', *Strategic Studies: A Reader*, T. Mahnken, J. Maiolo, eds. (New York: Routledge, 2008), 43–46.
52 Joel Rayburn, and Frank Sobchak, *The U.S. Army in the Iraq War, Volume I: Invasion, Insurgency, Civil War, 2003–2006* and *Volume II: Surge and Withdrawal, 2007–2011* (Carlisle: United States Army War College Press, 2019); British Army, *Operation HERRICK Campaign Study* (unpublished report, 2015).
53 Martijn Kitzen, 'The Netherlands' Lessons', *Parameters* 49:3 (2019), 52; Ben Barry, *Harsh Lessons: Iraq, Afghanistan and the Changing Character of War* (Abingdon: Routledge, 2017), 149.
54 1 (German/Netherlands) Corps, Factsheet Common Effort.
55 Ministry of Defence, 'Kamerbrief over de verwervingsvoorbereiding project MALE UAV' (*rijksoverheid.nl,* 8 June 2018).
56 Department of the Army, *Army Techniques Publication 3-96.1: Security Force Assistance Brigade'* (Washington, DC: Department of the Army, 2018).
57 Coombs, 'Canada's Lessons', *Parameters* 49:3 (2019), 39–40; Kitzen, 'The Netherlands' Lessons', 52–53; David Ucko, 'Systems Failure: the US Way of Irregular Warfare', *Small Wars & Insurgencies* 30:1 (2019), 223–226.
58 Murray, 'Innovation', 320; Martijn Kitzen, Sebastiaan Rietjens and Frans Osinga, 'Soft Power, the Hard Way: Adaptation by the Netherlands, Task Force Uruzgan', in *Military Adaptation in Afghanistan*, T. Farrell, F. Osinga, J. Russell, eds. (Stanford, CA: Stanford University Press, 2013), 186.
59 Jonathan Askonas, *A Muse of Fire: Why the U.S. Military Forgets What It Learns in War* (Oxford: St Cross College, 2019), 291.

References

Adamsky, Dimitry, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010).

Alderson, Alexander, '"Learn from Experience" or "Never Again"', *The RUSI Journal* 159:1 (2014), 40–48.

Argote, Linda, and Miron-Spektor, Ella, 'Organizational Learning: From Experience to Knowledge', *Organization Science* 22:5 (2010), 1123–1137.

Argyris, Chris, 'Double Loop Learning in Organizations', *Harvard Business Review* 55:5 (1977), 115–124.

Askonas, Jonathan D., *A Muse of Fire: Why the U.S. Military Forgets What It Learns in War* (Oxford: St Cross College, 2019).

Avant, Deborah D., 'The Institutional Sources of Military Doctrine: Hegemons in Peripheral Wars', *International Studies Quarterly* 37:4 (1993), 409–430.

Barry, Ben, *Harsh Lessons: Iraq, Afghanistan and the Changing Character of War* (Abingdon: Routledge, 2017).

Beckett, Ian F.W., *Modern Insurgencies and Counter-Insurgencies: Guerrillas and their Opponents since 1750* (London: Routledge, 2001).

Berends, Hans, and Antonacopoulou, Elena, 'Time and Organizational Learning: A Review and Agenda for Future Research', *International Journal of Management Reviews* 16 (2014), 437–453.

Berman, Eli, Felter, Joseph H., and Shapiro, Jacob N., *Small Wars, Big Data: The Information Revolution in Modern Conflict* (Princeton, NJ: Princeton University Press, 2018).

Betz, David, and Cormack, Anthony, 'Hot War, Cold Comfort: A Less Optimistic Take on the British Military in Afghanistan', *The RUSI Journal* 154:4 (2009), 26–29.

Biddle, Stephen, Friedman, Jeffrey A., and Shapiro, Jacob N., 'Testing the Surge: Why Did Violence Decline in Iraq in 2007?' *International Security* 37:1 (2012), 7–40.

Black, Jeremy, *Insurgency and Counterinsurgency: A Global History* (Lanham, MD: Rowman & Littlefield, 2016).

Bolger, Daniel P., *Why We Lost: A General's Inside Account of the Iraq and Afghanistan Wars* (Boston, MA: Mariner Books, 2015).

Brun, Itai, 'While You're Busy Making Other Plans'– The "Other RMA"', *Journal of Strategic Studies* 33:4 (2010), 535–565.

Burnes, Bernard, Cooper, Cary, and West, Penny, 'Organisational Learning: The New Management Paradigm?' *Management Decision* 41:5/6 (2003), 452–464.

Burton, Brian, and Nagl, John, 'Learning as We Go: the US Army Adapts to Counterinsurgency in Iraq, July 2004–December 2006', *Small Wars & Insurgencies* 19:3 (2008), 303–327.

Byrne, Barry, and Bannister, Frank, 'Knowledge Management in Defence', *Defence Forces Review* (2013), 71–93.

Carley, Kathleen M., and Harrald, John R., 'Organizational Learning Under Fire: Theory and Practice', *The American Behavioral Scientist* 40:3 (1997), 310–332.

Catignani, Sergio, 'Coping with Knowledge: Organizational Learning in the British Army?', *The Journal of Strategic Studies* 37:1 (2014), 30–64.

Catignani, Sergio, 'Getting COIN' at the Tactical Level in Afghanistan: Reassessing Counter-Insurgency Adaptation in the British Army', *Journal of Strategic Studies* 35:4 (2012), 513–539.

Clarke, Jason P., '"Good Allies": International Perspectives on Afghanistan', *The Strategy Bridge*. 29 March 2019. https://warroom.armywarcollege.edu/articles/good-allies/.

Cohen, Eliot A., and Gooch, John, *Military Misfortunes: The Anatomy of Failure in War* (New York: Free Press, 2006).

Cohen, Eliot, Crane, Conrad, Horvath, Jan, and Nagl, John, 'Principles, Imperatives and Paradoxes of Counterinsurgency', *Military Review* 86:2 (2006), 49–53.

Coombs, Howard G., 'Canada's Lessons', *Parameters* 49:3 (2019), 27–40.

Crane, Conrad C., *Cassandra in Oz* (Annapolis, MD: Naval Institute Press, 2016).

Crossan, Mary M., and Apaydin, Marina, 'A Multi-Dimensional Framework of Organizational Innovation: A Systemic Review of the Literature', *Journal of Management Studies* 47:6. (2010), 1154–1191.

Crossan, Mary M., Lane, Henry W., and White, Roderick E., 'An Organizational Learning Framework: From Intuition to Institution', *Academy of Management Review* 24:3(1999), 522–537.

Darling, Marilyn J., Guber, Heidi Sparkers, Smith, Jillaine S., and Stiles, James E.M., 'Emergent Learning: A Fraamework for Whole-System Strategy, Learning, and Adaptation', *The Foundation Review* 8:1 (2016), 59–73.

de Wijk, Rob, and Osinga, Frans, 'Military Innovation on a Shrinking Playing Field: Military Change in the Netherlands', in *A Transformation Gap? American Innovations and European Change*, Terry Terriff, Frans Osinga and Theo Farrell, eds., 108–143 (Stanford, CA: Stanford University Press).

De Winter, Sjoerd, *The Army after Afghanistan: A Case Study on Military Adaptation to Counterinsurgency Warfare within 12 Infantry Battalion Air Assault the Regiment Van Heutsz* (Breda: Netherlands Defence Academy (Master Thesis), 2015).

Defence, Department of, 2016 Defence White Paper (Canberra: Commonwealth of Australia, 2016).

Defence, Ministry of, 'Kamerbrief over de verwervingsvoorbereiding project MALE UAV', rijksoverheid.nl. 8 June 2018. Geopend September 26, 2019. https://webcache.googleusercontent.com/search?q=cache:mPitv2KO36EJ:https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/06/08/kamerbrief-over-de-verwervingsvoorbereiding-project-male-uav/kamerbrief-over-de-verwervingsvoorbereid.

Defense, United States Department of, *National Defense Strategy 2018* (Washington, DC: U.S. Department of Defense, 2018).

Dimitriu, George, Tuinman, Gijs, and van der Vorm, Martijn, 'Formative Years: Military Adaptation of Dutch Special Operations Forces in Afghanistan', *Special Operations Journal* 2:2 (2016), 146–166.

Doubler, Michael D., *Closing with the Enemy: How GIs Fought the War in Europe, 1944–1945* (Lawrence, KS: University Press of Kansas, 1994).

Dougherty, Deborah, 'Organizing for Innovation', in *Managing Organizations*, Stewart R. Clegg, Cynthia Hardy and Walter R. Nord, eds., 174–189 (London: SAGE Publications, 1999).

Downie, Richard Duncan, *Learning from Conflict: The U.S. Military in Vietnam, El Salvador, and the Drug War* (Westport, CT: Praeger, 1998).

Dyson, Tom, 'Organizing for Counter-insurgency: Explaining Doctrinal Adaptation in Britain and Germany', *Contemporary Security Policy* 33:1 (2012), 27–58.

Dyson, Tom, 'The Military as Learning Organisation: Establishing the Fundamentals of Best-practice in Lessons Learned', *Defence Studies* (2019), 1–23.

Edwards, Aaron, 'Misapplying Lessons Learned Analysing the Utility of British Counterinsurgency Strategy in Northern Ireland, 1971–76', *Small Wars & Insurgencies* 21:2 (2010), 303–330.

Egnell, Robert, 'Lessons from Helmand, Afghanistan: What Now for British Counterinsurgency?' *International Affairs* 87:2 (2011), 297–315.

Farrell, Theo, 'Introduction: Military Adaptation in War', in *Military Adaptation in Afghanistan*, Theo Farrell, Frans Osinga and James A. Russell, eds., 1–23 (Stanford, CA: Stanford University Press, 2013).

Farrell, Theo, Osinga, Frans, and Russell, James A., *Military Adaptation in Afghanistan* (Stanford, CA: Stanford Universty Press, 2013).

Farrel, Theo, and Terriff, Terry, *The Sources of Military Change: Culture, Politics, Technology* (Boulder, CO: Lynne Riener Publishers. 2002).

Finkel, Meir, *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield* (Stanford, CA: Stanford University Press, 2011).

Fiol, C. Marlene, and Lyles, Marjorie A., 'Organizational Learning', *The Academy of Management Review* 10:4 (1985), 803–813.

Fitzgerald, David, *Learning to Forget: US Army Counterinsurgency Doctrine and Practice from Vietnam to Iraq* (Stanford, CA: Stanford University Press, 2013).

Foley, Robert T., 'Dumb Donkeys or Cunning Foxes? Learning in the British and German Armies during the Great War', *International Affairs* 90:2 (2014), 279–298.

Foley, Robert T., Griffin, Stuart, and McCartney, Helen, '"Transformation in contact": Learning the Lessons of Modern War', *International Affairs* 87:2 (2011), 253–270.

Fox, Aimee, *Learning to Fight: Military Innovation and Change in the British Army, 1914–1918* (Cambridge: Cambridge University Press, 2018).

Freedman, Lawrence, *The Future of War: A History* (London: Penguin, 2017).

Fuller, J.R., and William, C., 'What Is a Military Lesson?' in *Strategic Studies: A Reader*, Thomas G. Mahnken and Joseph A. Maiolo, eds., 34–49 (New York: Routledge, 2008).

Ganz, Scott G., 'Ignorant Decision Making and Educated Inertia: Some Political Pathologies of Organizational Learning', *Organization Science* 29:1 (2018), 39–57.

Gentile, Gian P., 'A (Slightly) Better War: A Narrative and Its Defects', *World Affairs* 171:1 (2008), 57–64.

Gentile, Gian P., 'A Strategy of Tactics: Population-centric COIN and the Army', *Parameters* 39:3 (2009), 5–17.

Goldman, Emily O., and Andres, Richard B., 'Systemic Effects of Military Innovation and Diffusion', *Security Studies* 8:4 (1999), 79–125.

Government, HM, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* (London, 2015).

Grah, Barbara, Dimovski, Vlado, Snow, Charles C., and Peterlin, Judita, 'Expanding the Model of Organizational Learning: Scope, Contingencies, and Dynamics', *Economic and Business Review* 18:2 (2016), 183–212.

Griffin, Stuart, 'Military Innovation Studies: Multidisciplinary or Lacking Discipline', *The Journal of Strategic Studies* 40:1–2 (2017), 196–224.

Grissom, Adam, 'The Future of Military Innovation Studies', *The Journal of Strategic Studies* 29:5 (2006), 905–934.

Gudmundsson, Bruce I., *Stormtroop Tactics'Innovation in the German Army, 1914–1918* (New York: Praeger, 1989).

Haaland, Torunn Laugen, 'The Limits to Learning in Military Operations: Bottom-up Adaptation in the Norwegian Army in Northern Afghanistan, 2007–2012', *The Journal of Strategic Studies* 39:7 (2016), 999–1022.

Harkness, Kristen A., and Hunzeker, Michael, 'Military Maladaptation: Counterinsurgency and the Politics of Failure', *Journal of Strategic Studies* 38:6 (2015), 777–800.

Hasselbladh, Hans, and Yden, Karl, 'Why Military Organizations Are Cautious About Learning?', *Armed Forces & Society* 46:3 (2020), 475–494.

Heuser, Beatrice, and Shamir, Eitan, *Insurgencies and Counterinsurgencies: National Styles and Strategic Cultures* (Cambridge: Cambridge University Press, 2016).

Heuser, Beatrice, and Shamir, Eitan, 'Universal Toolbox, National Styles or Divergence of Civilisations?' in *Insurgencies and Counterinsurgencies: National Styles and Strategic Cultures*, Beatrice Heuser and Eitan Shamir, eds., 332–370 (New York: Cambridge University Press, 2016).

Hill, Andrew, and Gerras, Stephen, 'Systems of Denial', *Naval War College Review* 69:1 (2016), 109–132.

HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* (London, 2015).

Hoffman, Frank G., *Learning While Under Fire: Military Change in Wartime* (London: King's College, Doctoral Dissertation, 2015).

Hoffman, Frank G., 'Neo-Classical Counterinsurgency', *Parameters* 41:4 (2011–2012), 1–17.

Hoiback, Harald, 'The Anatomy of Doctrine and Ways to Keep It Fit', *The Journal of Strategic Studies* 39, 2 (2016), 185–197.

Huysman, Marleen, 'An Organizational Learning Approach to the Learning Organization', *European Journal of Work and Organizational Psychology* 9:2 (2000), 133–145.

Jensen, Benjamin M., *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford, CA: Stanford University Press, 2016).

Johnson, David, 'Failure to Learn: Reflections on a Career in the Post-Vietnam Army', *War on the Rocks* 24 January 2014. Geopend August 23, 2019. https://warontherocks.com/2014/01/failure-to-learn-reflections-on-a-career-in-the-post-vietnam-army/.

Johnson, David E., 'You Go to Coin with the Military You Have', in *Insurgencies and Counterinsurgencies: National Styles and Strategic Cultures*, Beatrice Heuser and Eitan Shamir, eds., 113–148 (Cambridge: Cambridge University Press, 2016).

Kaplan, Fred, 'The of the Age of Petraeus: The Rise and Fall of Counterinsurgency', *Foreign Affairs* 92:1 (2013), 75–90.

Kilcullen, David, *Blood Year: The Unravelling of Western Counterterrorism* (New York: Oxford University Press, 2016).

Kilcullen, David, 'Counterinsurgency: The State of a Controversial Art', in *The Routledge Handbook of Insurgency and Counterinsurgency*, Paul B. Rich and Isabelle Duyvesteyn, eds., 128–153 (London: Routledge, 2012).

Kim, Daniel H.,'The Link between Individual and Organizational Learning', *Sloan Management Review* 35:1 (1993), 37–50.

Kitzen, Martijn, *The Course of Co-option: Co-option of Local Power-holders as a Tool for Obtaining Control Over the Population in Counterinsurgency Campaigns in Weblike Societies* (Breda: Netherlands Defence Academy, 2016).

Kitzen, Martijn, 'The Netherlands' Lessons', *Parameters* 49:3 (2019), 41–53.

Kitzen, Martijn, 'Western Military Culture and Counterinsurgency: An Ambiguous Reality', *Scientia Militaria* 40:1 (2012), 1–24.

Kitzen, Martijn, Rietjens, Sebastiaan, and Osinga, Frans, 'Soft Power, the Hard Way: Adaptation by the Netherlands, Task Force Uruzgan', in *Military Adaptation in Afghanistan*, Theo Farrell, Frans Osinga and James A. Russell, eds., 159–191 (Stanford, CA: Stanford University Press, 2013).

Kjellstrom Elgin, Katherine, and Gilbert, Peter, 'How the Army Is (not) Preparing for the Next War.' *The War Room* 25 September 2019. Accessed September 26, 2019. https://warroom.armywarcollege.edu/articles/the-next-war/.

Kollars, Nina, *By the Seat of Their Pants: Military Technological Adaptation in War* (Columbus, OH: The Ohio State University, 2012).

Kollars, Nina, 'Genius and Mastery in Military Innovation', *Survival* 59:2 (2017), 125–138.

Kollars, Nina, 'Military Innovation's Dialectic: Gun Trucks and Rapid Acquisition', *Security Studies* 23:4 (2014), 787–813.

Kollars, Nina, 'Organising Adaptation in War', *Survival* 57:6 (2015), 111–126.

Kollars, Nina A., 'War's Horizon: Soldier-Led Adaptation in Iraq and Vietnam', *The Journal of Strategic Studies* 38:4 (2015), 529–553.

Ledwidge, Frank, *Losing Small Wars* (New Haven, CT: Yale University Press, 2017).

Levinthal, Daniel A., and March, James G., 'The Myopia of Learning', *Strategic Management Journal* 14 (1993), 95–112.

Long, Austin, *Doctrine of Eternal Recurrence: The U.S. Military and Counterinsurgency Doctrine, 1960–1970 and 2003–2006* (Santa Monica, CA: RAND Corporation, 2008).

Long, Austin, *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the US and UK* (Ithaca, NY: Cornell University Press, 2016).

Luttwak, Edward N., 'Dead End: Counterinsurgency Warfare as Military Malpractice', *Harper's Magazine* 314:1881 (2007), 33–42.

Mains, Steven, and Ariely, Gil Ad, 'Learning While Fighting: Operational Knowledge Management that Makes a Difference', *PRISM* 2:3 (2011), 165–176.

March, James G., 'Exploration and Exploitation in Organizational Learning', *Organization Sccience* 2:1 (1991), 71–87.

Marcus, Raphael D., 'Military Innovation and Tactical Adaptation in the Israel-Hizballah Conflict: The Institutionalization of Lesson-Learning in the IDF', *The Journal of Strategic Studies* 38:4 (2015), 500–528.

Moyar, Mark, *A Question of Command: Counterinsurgency from the Civil War to Iraq* (New Haven, CT: Yale University Press, 2009).

Murray, Williamson, 'Innovation: Past and Future', in *Military Innovation in the Interwar Period*, Williamson Murray and Allan R. Millet, eds., 300–328 (New York: Cambridge University Press, 1996).

Murray, Williamson, *Military Innovation in the Interwar Period* (Cambridge: Cambridge University Press, 1996).

Nagl, John A., *Knife Fights: A Memoir of Modern War in Theory and Practice* (Penguin: New York, 2014).

Nagl, John A., *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: Chicago University Press, 2002).

Nolan, Cathal J., *The Allure of Battle* (Oxford: Oxford University Press, 2017).

Noll, Joerg, and Rietjens, Sebastiaan, 'Learning the Hard Way: NATO's Civil-military Cooperation', in *Theorising NATO: New Perspective on the Atlantic Alliance*, Mark Webber and Adrian Hyde-Price, eds., 223–242 (London: Routledge, 2016).

Nonaka, Ikujiro, 'The Knowledge-Creating Company', *Harvard Business Review* (1991), 96–104.

Nonaka, Ikujiro, and Konno, Noboru, 'The Concept of "Ba": Building a Foundation for Knowledge Creation', *California Management Review* 40:3(1998), 40–54.

Nonaka, Ikujiro, and Toyama, Ryoko, 'The Knowledge-creating Theory Revisited: Knowledge Creation as a Synthesizing Process', *Knowledge Management Research & Practice* 1(2003), 2–10.

Nonaka, Ikujiro, and von Krogh, Georg, 'Perspective—Tacit Knowledge and Knowledge Conversion: Controversy and Advancement in Organizational Knowledge Creation Theory', *Organization Science* 20:3 (2009), 635–652.

Osinga, Frans, *Science, Strategy and War: The Strategic Theory of John Boyd* (Delft: Eburon Academic Publishers, 2005).

O'Toole, Paddy, and Talbot, Steven, 'Fighting for Knowledge: Developing Learning Systems in the Australian Army', *Armed Forces & Society* 37:1 (2011), 42–67.

Packer, George, 'The Lesson of Tal Afar', *The New Yorker*, 10 April 2006.

Porch, Douglas, *Counterinsurgency: Exposing the Myths of the New Way of War* (New York: Cambridge University Press, 2013).

Porch, Douglas, 'The Dangerous Myths and Dubious Promise of COIN', *Small Wars & Insurgencies* 22:2 (2011), 239–257.

Porter, Patrick, 'Goodbye to All that: On Small Wars and Big Choices', *Small Wars & Insurgencies* 25:3 (2014), 685–695.

Posen, Barry R., *The Sources of Military Doctrine: France, Britain and Germany between the World Wars* (Ithaca, NY: Cornell University Press, 1984).

Rayburn, Joel D., and Sobchak, Frank K., *The U.S. Army in the Iraq War, Volume I: Invasion, Insurgency, Civil War, 2003–2006* (Carlisle: United States Army War College Press, 2019).

Rayburn, Joel D., and Sobchak, Frank K., *The U.S. Army in the Iraq War, Volume II: Surge and Withdrawal, 2007–2011* (Carlisle: United States Army War College Press, . 2019).

Riddle, Bryan, *Essence of Desperation* (Lanham, MD: Lexington Books, 2018).

Rosen, Stephen Peter, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991).

Russell, James A., *Innovation, Transformation and War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005–2007* (Stanford, CA: Stanford University Press, 2011).

Sangar, Eric, 'The Pitfalls of Learning from Historical Experience: The British Army's Debate on Useful Lessons for the War in Afghanistan', *Contemporary Security Policy* 37:2 (2016), 223–245.

Scales, John, 'Thoughts as I Watch My Army Walk Away from Counterinsurgency Once Again', *Foreign Policy*, 11 February 2016.

Schmitt, Olivier, 'French Military Adaptation in the Afghan War: Looking Inward or Outward', *The Journal of Strategic Studies* 40:4 (2017), 577–599.

Serena, Chad C., *A Revolution in Military Adaptation: The US Army in Iraq* (Washington, DC: Georgetown University Press, 2011).

Shimko, Keith L., *The Iraq Wars and America's Military Revolution* (New York: Cambridge University Press, 2010).

Shurkin, Michael, *France's War in Mali: Lessons for an Expeditionary Army* (Santa Monica, CA: RAND Corporation, 2014).

Sinterniklaas, Rob, *Military Innovation: Cutting the Gordian Knot* (Breda: Faculty of Military Sciences, Netherlands Defence Academy, 2018).

South, Todd, 'Army's Detailed Iraq War Study Remains Unpublished Years After Completion', *Army Times* 25 October 2018. Accessed September 5, 2019. https://www.armytimes.com/news/your-army/2018/10/25/armys-detailed-iraq-war-study-remains-unpublished-years-after-completion/.

Taber, Robert, *War of the Flea: The Classic Study of Guerrilla Warfare* (New York: L. Stuart, . 1965).

Ten Cate, Arthur, and Zaalberg, Thijs Brocades, *A Gentle Occupation* (Leiden: Leiden University Press, 2014).

Ucko, David H., 'Critics Gone Wild: Counterinsurgency as the Root of all Evil', *Small Wars & Insurgencies* 25:1 (2014), 161–179.

Ucko, David H., 'Systems Failure: The US Way of Irregular Warfare', *Small Wars & Insurgencies* 30:1 (2019), 223–254.

Ucko, David H., *The New Counterinsurgency Era* (Washington, DC: Georgetown, 2009).

Ucko, David H., 'Whither Counterinsurgency', in *The Routledge Handbook of Insurgency and Countrinsurgency*, Paul B. Rich and Isabelle Duyvesteyn, eds., 67–79 (London: Routledge, 2012).

Ucko, David H., and Marks, Thomas A., 'Violence in Context: Mapping the Strategies and Operational Art of Irregular Warfare', *Contemporary Security Policy* 39:2 (2018), 206–233.

United States Department of the Army, *FM 3–24: Counterinsurgency Field Manual* (Chicago: Chicago University Press, 2007).

U.S. Army Training and Doctrine Command, *Multi Domain Battle: Evolution of Combined Arms for the 21st Century, 2025–2040* (Fort Eustis: TRADOC, 2017).

van Wiggen, Otto P., and Aarten, R.J., 'Oefening Bison Drawsko 2017: Een essentiële nulmeting voor de Landmacht', *Militaire Spectator* 186:12 (2017), 581–596.

Waldman, Thomas, 'Vicarious Warfare: The Counterproductive Consequences of Modern American Military Practice', *Contemporary Security Policy* 39:2 (2018), 181–205.

Weick, Karl E., and Westley, Frances, 'Organizational Learning: Affirming an Oxymoron', in *Managing Organizations*, Stewart R. Clegg, Cynthia Hardy and Walter R. Nord, eds., 190–208 (London: SAGE Publications, 1999).

Wiggen, Otto van and Aarten, Robert-Jan, 'Oefening Bison Drawsko 2017: Een essentiële nulmeting voor de Landmacht', *Militaire Spectator* 186:12 (2017), 581–596.

Wijk, Rob de and Osinga, Frans, 'Military Innovation on a Shrinking Playing Field: Military Change in the Netherlands', in *A Transformation Gap? American Innovations and European Change*, Terry Terriff, Frans Osinga, and Theo Farrell, eds., 108–143 (Stanford, CA: Stanford University Press, 2010).

Winter, Sjoerd de, *The Army after Afghanistan: A Case Study on Military Adaptation to Counterinsurgency Warfare within 12 Infantry Battalion Air Assault the Regiment Van Heutsz* (Breda: Netherlands Defence Academy, 2015).

Part VI

Law and war

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

13 Fighting a war without violence

The rules of International Humanitarian Law for military cyber-operations below the threshold of 'attack'

Bart van den Bosch

Introduction

Future warfare will most likely not follow the cleavages that states and lawmakers traditionally use to regulate and control the seemingly infinite complexity of human societies. Consider the fight against Islamic State that was fought on the territory of Syria and Iraq by a coalition of states. For International Humanitarian Law (IHL) it makes a significant difference whether the conflict is classified as an international or a non-international armed conflict. In an international armed conflict, captured combatants are granted a prisoner of war status, while in a non-international armed conflict fighters might be criminally prosecuted for their engagements. Another example is the so-called 'war on terror' which the United States of America launched after the 9–11 attacks in 2001. Initially it was clearly an international armed conflict fought by the United States and its allies against Afghanistan where the Taliban government harboured Al-Qaeda. It became slightly obscured when the Taliban was defeated and even more when the United States decided to expand the 'war on terror' outside Afghanistan. Was there still an armed conflict ongoing and if so against whom? From a legal point of view essential questions since IHL is only applicable during an armed conflict.

To make matters even more complex distinctions between a party's Diplomatic Information Military Economic Financial Information and Legal (DIMEFIL) powers have become increasingly blurred and sometimes even are undefinable.[1] Moreover, modern conflicts might involve both public and private entities with very different agendas and who, through modern technology, are capable of projecting their power over time and distance. This decline of 'natural' barriers results in a diminishing role for physical borders and complicates the use of territorial-based notions like sovereignty or – more military – control over an area. Because of the consecutive lack of clarity, such conflicts are sometimes referred to as ambiguous or grey zone warfare.[2] The ramifications of this emerging reality are being felt by both practitioners and academics. Whereas the latter are engaged in a debate on which paradigm fits this situation best, the former have to deal

with uncertainty over which measures to take and what rules to follow. This contribution aims at providing new scholarly insights while simultaneously offering military commanders solutions that can be applied to the conduct of war.

Before analysing conflicts in the grey zone from a legal perspective it is essential to realize that there exists no such a thing as a single set of rules – what is normally referred to as a legal regime – regulating this type of warfare. There are all kind of legal regimes but they are all shaped in accordance with traditional distinctions. There is, for instance, a regime for peace and another for war. There are rules for national issues, but international problems are solved following different rules. From a legal point of view, the different regimes, each with own rules and mostly also with a unique vocabulary, are clearly separated by rigid watersheds. This, however, also implies that the same word or expression can have a specific meaning in a certain regime but a different meaning in another. For instance, attack in 'armed attack' as mentioned in article 51 of the Charter of the United Nations has a different meaning and connotation than 'attack' in IHL. Consequently, one has to be clear about the meaning of a term in a specific legal regime before even trying to take the discussion up to the level of covering multiple regimes as is the case in grey zone warfare.

A most urgent example, in this regard, is the term cyberattack. For the military fighting a war, the legal paradigm is IHL also known as the Law of Armed Conflict (LOAC). New technologies, especially the development of the cyber domain, have created a number of possibilities to fight a war with lethal but even more with non-lethal means and methods. IHL deals extensively with the former but is ostensibly silent on the latter. This can be explained by the fact that IHL has developed over many years with the two-fold purpose of regulating hostilities (including the limitation of permitted methods and means of warfare), and protecting those persons and objects that do not or no longer participate in armed conflicts. To achieve these goals, the main focus has been on the reduction of the horrors of war. This has resulted in a focus on 'attacks', a specific category of military operations that is defined as 'acts of violence against the adversary, whether in offence or in defence'.[3] A direct consequence of the focus on attacks is the relative lack of attention for military operations that do not meet the conditions of 'attack' as prescribed by IHL.

The rapid development of the cyber domain has rendered both the military and society as a whole increasingly dependent on non-physical elements such as data and computer programs. For armed conflicts this opens up a whole range of possibilities for 'non-violent' operations, or operations below the threshold of 'attack' as understood by IHL. This urges for a better understanding of what exactly encompasses a cyberattack, and when an operation is staying below this threshold. Furthermore, clarification is needed about the extent and way in which the rules IHL apply to these (cyber)operations not reaching the level of 'attack'. Although it is generally accepted that IHL

is applicable in the cyber domain, the exact implementation of existing rules has been subject of a fierce debate.[4] In the case of cyberattacks this has resulted in two main points of view, the so-called permissive and the restrictive school, respectively.[5] This chapter introduces a theory that combines both schools by preserving their strong and overcoming their weak points which allows for formulating practical guidelines for implementing IHL in military (cyber)operations below the threshold of attack.[6] In addition, this novel theoretic approach towards IHL also offers a new starting point for the discussion on what legal regime or regimes best fit grey zone warfare.

What is a cyberattack below the threshold of 'attack'?

Before tackling the specific topic of cyberattack, the threshold of 'attack' in the traditional military meaning has to be defined explicitly. As indicated earlier, attacks are defined as 'acts of violence against the adversary, whether in offence or in defence'.[7] Many of the IHL rules that are recognized in both treaty and customary law are constructed around the term 'attacks'. Examples include the prohibition to attack civilians, civilian objects, medical personnel, etc. Almost no rules can be found for military operations that are not 'attacks', although it is widely accepted that these operations exist. A reconnaissance operation, an intelligence operation or electronic and psychological warfare are examples of military operations that help to win an armed conflict. These operations could, and should in the author's opinion, be qualified as 'methods and means of warfare'. If mentioned operations are planned and executed with the intention of degrading the military capabilities of an opponent during an armed conflict they have the same objective as a physical attack. They are intended to contribute to the successful ending of the armed conflict. Not considering them as 'methods and means of warfare' would be a *contradictio in terminis*.[8] Nevertheless, they are not considered 'attacks' as defined under IHL.

The key reason why these military operations are not being considered 'attacks' is that they are not aimed at, nor result in physical injury or damage.[9] Hence, all military activities that do not seek or result in physical consequences per definition take place below the threshold of 'attack'. This explanation of the threshold of attack on the basis of physical consequences is basically non-contentious when applied to so-called kinetic warfare which is all about physically destroying the opponent. This unambiguity changes when entering the rather murky arena of cyberwarfare. What if you manage to disable an enemy radar station by hacking it and alter some computer program necessary to operate it correctly? Since no physical damage has been done, does such an operation not qualify as an attack? Does it make a difference if the system is disabled for minutes or permanently? Does it make a difference when the radar system is still functioning and is only partially disabled by, for instance, losing its ability to register a certain kind of airplanes?

Two schools of thought have evolved in response to this type of questions. At the basic level, both opposing views agree that only if a military operation qualifies as an 'attack' it has to follow the rules that IHL provides for 'attacks'. Moreover, they also share the implicit assumption that IHL does not prescribe rules for activities that lie below the threshold of attack.[10] But what about the differences? First, the permissive school reasons that as long as there is no physical destruction, there has not been an attack.[11] The consequence of this rationale is that military operations that do not cause such destruction do not have to follow the constraining rules governing 'attacks'. This opens up a range of possible objects that can be legally targeted – not attacked – within the regime of IHL, hence the name 'permissive'. Examples are countless but some of the most notable include websites, social media accounts and bank accounts, all of which are not necessarily related to combatants. It should be noted, therefore, that such objects belonging to relatives, friends and others that can be exploited to reach a specific military goals fall within the outreach of targetable objects.

On the other hand, the restrictive school follows the line of reasoning that it does not matter how an object is disabled, by total or partial destruction, by capture or neutralization.[12] Instead it is the result that matters; if an operation renders an object no longer capable of fulfilling the function it was intended to do, that operation qualifies as an 'attack'. The result is that far more operations have to follow the rules regulating attacks, hence the name 'restrictive'. In this reasoning any operation against a civilian object is seen as an attack and therefore forbidden. For instance, the temporary shut down of a press website to postpone a message from becoming public for 30 minutes would be considered a forbidden attack and following that reasoning a breach of IHL or in lay terms, a war crime.

The problem with both schools is that the permissive school is generally seen as too permissive while the restrictive school is considered too restrictive. An attempt to find middle ground is the so-called functionality test which is designed to assess the effects of a military operation on the functionality of a targeted (weapon) system. This

> appropriately addresses fair criticism that the permissive approach fails to adequately constrain the effects of cyber operations on the civilian population. At the same time, it adds a degree of clarity as to where the threshold of attack lies that is missing in the restrictive approach.[13]

The problem with this functionality test, however, is that it leaves more or less the same questions unanswered. When is the functionality of a system lost? Does it make a difference if it is only disturbed and is still functioning slower or only partially? Was it an attack if just restarting the system solves the problem?

Despite their differences, both schools agree that there is a generally accepted notion that if a cyber-operation leads to physical consequences,

i.e. something is physically broken or someone gets physically hurt, it definitely qualifies as an 'attack'. Because IHL protects extensively against 'attacks' the restrictive school aims at a broad interpretation of 'attack' including non-physical damage, while the permissive school seeks to limit the regulating rules by reasoning that operations without physical effects are not 'attacks'. This points at the fact that a solution for providing more clarity on the exact status of non-kinetic operations lies in enhancing consensus between both schools of thought. Such a solution can be found in abandoning the interpretation that IHL only regulates 'attacks' and accept the interpretation that IHL also is applicable to military operations below the threshold of attack. This novel approach takes the heat out of the discussion on where the exact threshold of attack lies, because this is no longer relevant; even when an operation is below the threshold, it still has to fulfil IHL requirements. Thereby the restrictive school's argument to reject the physical consequences criterion (as whole range of targets would escape the regulatory reach of IHL) is no longer valid because the protective umbrella of IHL also applies below the threshold of 'attack'. Therefore, there is no longer a need for expanding the definition of attack beyond physical consequences, so the common understanding between the schools that military operations with physical consequences are 'attacks' in any case can serve as the threshold for 'attack'.

The physical consequences criterion has the advantage that it is clear, easy to validate and already well-accepted in kinetic warfare. Additional advantage is that because the unchanged threshold of attack, all military operations (cyber and more traditional operations like psychological or electronic operations) below the threshold of attack can be treated equally when it comes to application of IHL.

Rules in IHL below the threshold of attack

In order to understand how IHL can be applied below the threshold of attack, it is first necessary to have a closer look at the theoretical base of this rather new interpretation. In IHL there is a distinction between attacks and other military operations. This follows directly from the linguistic argument that the main IHL treaties explicitly make a difference between the two and is also supported by the way states explain and practice IHL.[14] There is also a general acceptance that those military operations in IHL are, in the same way as attacks, part of the broader concept called 'warfare'. Both treaty and customary law recognize that the methods and means of warfare are not unlimited and that if there are no specific rules available to a certain situation, there is a legal safety-net most commonly known as the Martens-Clause.[15]

This clause states that 'civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the

dictates of public conscience'.[16] This well-established legal safety-net makes that, despite the lack of a set of specific rules, military operations below the threshold of attack when used as a method or means of warfare still have to fulfil the protective principles of IHL. This means that a return to the principles is necessary for applying IHL below the threshold of attack. This is common practice in international law as these principles are recognized as one of its sources.[17] These principles 'provide the normative framework upon which the entire system of rules is based' and can be used 'as aids in interpretation and as means to fill gaps and ensure coherence'.[18] As stated before one can say that the purpose of IHL is twofold. On the one hand it regulates hostilities, which includes imposing limitations on permitted methods and means of warfare. On the other hand, IHL protects persons that do not or no longer participate in hostilities, as well as objects which do not have a direct military value in armed conflicts. To achieve this twofold purpose, IHL is constructed around two primary principles, military necessity and humanity. These are the two principles of international law that provide protection and authority even when no specific rules are available. IHL defines a balance between those primary principles or in more pragmatic terms, it sets the rules to win a war, while simultaneously reducing the horrors of war. It is important to realize that these principles more often than not point in opposite directions; whereas operations that ignore humanity might prove military very successful, military actions that seek to avoid all human losses would probably never bring military success. This is why the metaphor of a balance is commonly used.

To strike a balance between these primary principles some additional principles have been recognized such as, among others, distinction, proportionality, unnecessary suffering, precautions, limitation and chivalry.[19] How these principles relate to each other is not always explained in a clear and unambiguous way. Sometimes the rules regarding precautions, for instance, are said to be the result of distinction and not an independent principle of IHL. Another example concerns the rule that prohibits unnecessary suffering, which is said to follow from the principle of humanity. These different interpretations of whether a principle is independent or derivative from another explains why for instance Van den Boogaard in the next chapter refers to distinction, precautions and proportionality as leading principles. This analysis follows the principles adhered to by the Netherlands, being military necessity, humanity, distinction, proportionality and chivalry, which are 'generally accepted' to form the fundamental basis for the whole structure of IHL.[20]

How do these principles apply to military (cyber-)operations below the threshold of attack, or in other words, (cyber-)operations that do not have physical consequences? To start with, the principle of military necessity can be applied equally to attacks and military operations below the threshold of attack. If there is no military advantage to gain, IHL explicitly forbids these operations.[21] The other primary principle, humanity, is a more overarching principle. It serves at the basis and therefore effects the other principles.

Balancing military necessity with humanity can be done in the same way as done with attacks. There it results in the so-called proportionality rule meaning that an attack is forbidden when 'the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.[22] The outcome, however, is probably different, because the negative impact on humanity will most likely be less severe for military operations without physical consequences than for attacks with physical injuries and possible deaths. Being killed or physically injured has a bigger impact on someone's life than not being able to access a Facebook-account for a period of time. The latter most likely has a negative impact on someone's life which means that when it is caused by a military operation, there has to be a military advantage to balance this negative impact to fulfil the LOAC principles. However, the advantage can be smaller or less direct to be considered as sufficiently counterweigh the negative impact or in balancing terms, the result is that a balance might be found with less military advantage.

Next, the principle of distinction leads to different outcomes when applied to military operations below the threshold of attack. LOAC provides general protection against attacks for both civilian persons and civilian objects. Below the threshold, there are however variations in protection between persons and objects. As far as general protection of the civilian population is concerned, attacks are forbidden. Military operations below the threshold, however, may be directed at the civilian population as long as this population is not exposed to physical dangers arising from military operations.[23] For civilian objects, the difference in protection between attacks and other military operations is greater. Civilian objects, with the exception of certain categories, do not enjoy a general protection against military operations. Military operations may not only be directed at civilian objects, civilian objects may also be used for military operations even if this means that they are exposed to the risk of damage or destruction. A practical example may clarify this. A military unit that wants to move from A to B (a military operation below the threshold of attack) needs to cross a river. There is a bridge over that river normally only used for civilian traffic. The unit can use this bridge, even knowing that this use renders the bridge a military objective for the opponent according to the rules of IHL.[24] The operation, thereby, deliberately endangers the bridge to possible enemy attack which might result in physical damage or even destruction.

When applying the following principle of proportionality to below threshold operations it is pivotal to distinguish between proportionality as a principle and the so-called proportionality rule in IHL. The latter rule is seen as the codification of the aforementioned balance between military necessity and humanity, and is reserved for attacks. As the key balancing principle between the IHL's primary principles, however, proportionality might be applied to other military operations as well – as will be shown in the last part of this chapter.

Last, chivalry in IHL has a somewhat different status compared to the other principles. As a principle it can play a legal role in the interpretation of existing rules, for instance in judging whether or not perfidy is prohibited.[25] Besides this legal role, it can make a contribution to moral or operational problems.[26] In this last sense, the principle of chivalry will not result in binding legal obligations neither for attacks nor for operations below the threshold.

Where does this analysis of the principles of IHL when applied to (cyber-) operations below the threshold of attacks leads us in the absence of specific rules for this kind of operations? Overall, two overarching rules can be identified. The first considers a deliberation with the purpose of balancing the fundamental principles of military necessity and humanity. The other IHL principles play a supporting role in this deliberation. This rule is formulated as follows: the non-physical consequences of a military (cyber-)operation for the civilian population, individual civilians, civilian objects or a combination thereof should not be excessive in relation to the anticipated military advantage. The wording of this rule heavily leans on the earlier mentioned proportionality rule for attacks but the level of military advantage necessary to balance the deliberation is lower.[27] For instance indirect or less concrete military advantage like public support for a military operation may also be calculated. Choosing the same kind of wording expresses the resemblance with the proportionality rule for attacks and thereby provides guidance to military commanders and others that have to make this deliberation. The actual application of this deliberation, therefore, benefits from existing training and previous experiences of military commanders with regard to the use of the proportionality rule.[28]

The second identified rule is the obligation that during planning, preparation and execution of an (cyber-)operation below the threshold of attack 'everything feasible' should be done to exclude that the (cyber-)operation will or could have physical consequences. This obligation has the purpose to avoid the possibility that a lawful (cyber-)operation transforms into a (possible) illegal attack. What should be understood by 'everything feasible' is depending on all circumstances at the time and should be interpreted in good faith and with common sense, sometimes referred to as the standard of the 'reasonable military commander'.[29] To be able to fulfil this criterion it is obvious that at least the commander should have a clear understanding of the effects the operation will have on the targeted system. A good knowledge of that system, including connections with other systems, working of the system and security levels, is probably always necessary. If time and resources are available, perhaps a simulation of the operation in a laboratory environment is a possibility to lower the risks. If during the planning, preparation or execution of the (cyber-)operation it becomes clear that physical consequences cannot be excluded the operation should be treated as an attack and therefore judged by the more strict rules regarding such an act.

When applied properly, both rules allow parties to the conflict to perform the military missions below the threshold of attack necessary to win the conflict and at the same time respect the regulatory and protective umbrella of IHL. With this certainty the operations below the threshold can become an even more attractive alternative for attacks. These operations should at least be considered when deciding upon a course of action to follow.

Conclusion

Embracing the view that IHL is also applicable below the threshold of attack opens up the possibility to close the gap in the academic debate between the restrictive and the permissive approach to cyber-operations. Two rules can then be identified for cyber-operations below the threshold of attack: a proportionality deliberation and precautions obligation. These two rules provide pragmatic, applicable guidance for military commanders. Applying these rules assures that the cyber-operations fulfil the requirements of IHL both in situations it is clear that an armed conflict exists and in situations where there might be uncertainty over the status of a conflict, the grey zone warfare. The view that IHL is applicable below the threshold of attacks is not necessarily limited to cyber-operations. The identified rules can be applied to all non-destructive military operations like information-campaigns or disturbing operations like jamming. The legal certainty provided by this conclusion can, and probably will for those states that take international law seriously, contribute to the awareness that military operations below the threshold of attack can be a valuable and realistic alternative for attacks.

The ambiguity between peace and war is likely to feature in both current and upcoming conflicts. This legally undefined reality offers opportunities especially for military operations below the threshold of attack. Their appearance, therefore, will most likely increase both in a quantitative and qualitative way. Although IHL is the legal regime for war, being able to apply this regime to military operations that are at the low end of the violence spectrum (or at the high end of the peacetime spectrum) is at least a step forward in legally regulating the undefined but therefore no less realistic situations of grey zone warfare.

Notes

1 See for instance NATO, *Brussels Summit Declaration* (Brussels: NATO, 2018), par.21.
2 The term grey zone warfare is much-used but has never been defined authoritatively. Hence, some even object the concept because it is unclear and confusing. The reference to grey zone warfare is therefore useful to express unclearness.
3 ICRC, *Additional Protocol I to the Geneva Conventions* (*API*) (Geneva: ICRC, 1977), art. 49 (1).
4 See for instance Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Security, *Transmits*

Report A/68/98 (New York: UN, 2013), par. 20. Michael Schmitt ed., *Tallinn Manual on the International Law applicable to Cyber Warfare* (Cambridge: Cambridge University Press 2013), 5, Jean Marie Henckaert and Louise Doswald-Beck, *Customary International Humanitarian Law, Volume I: Rules* (Cambridge: Cambridge University Press 2005), xxxvi.

5 Michael Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack', *International review of the Red Cross* 96:893 (2014), 189–206.

6 This theory is based upon the author's PhD research. See Bart van den Bosch, *Oorlog voeren zonder geweld* (Amsterdam: Amsterdam University, 2019), https://dare.uva.nl/search?identifier=8c79d32a-8568-41a2-a4f0-00df37ca6a87.

7 ICRC, *API*, art 49 (1).

8 ICRC, *API*, art 35.

9 A shot which misses, but was aimed with the intention to kill a person thus still qualifies as an 'attack'.

10 Schmitt, *Tallinn Manual*, 59: 'would potentially escape the regulatory reach of the law of armed conflict'. Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law', *Israel Law Review* 48:1 (2015), 78 'many targets whose physical equivalents are firmly protected by IHL from enemy combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace'.

11 The terms 'permissive' and 'restrictive' were first introduced in Michael Schmitt, 'Wired Warfare: Computer network attack and *jus in bello*', *International Review of the Red Cross* 84:846 (2002), 365–399. Schmitt himself supports the permissive school.

12 Most prominent supporter of this school is Knut Dörmann, see Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', in Karin Bystrom, ed., *Proceedings of the International Experts Conference on Computer Network Attacks and the Applicability of International Humanitarian Law* (Stockholm: Swedish National Defence College, 2005).

13 Michael Schmitt, 'Rewired Warfare', 189–206.

14 See for instance ICRC, *API*, art 51 (1), 'The civilian population and individual civilians shall enjoy general protection against dangers arising from military *operations*' and art 51 (2), 'The civilian population as such, as well as individual civilians, shall not be the object of *attack*' (emphasis by author). Despite the absolute prohibition on attacking the civilian population, these rules are generally interpreted to permit, for example, information operations intended to influence the civilian population for withdrawing support to military forces (with the objective that the military ultimately stop their fighting).

15 For treaty law see ICRC, *API*, art 35 (1). The Martens-Clause is named after a Russian diplomat at the Hague Peace Conference of 1899.

16 ICRC, *API*, art. 1 (2).

17 United Nations, *Statute of the International Court of Justice* (San Francisco, CA: United Nations, 1945), art. 38 (1) c.

18 Terry Gill, 'Chivalry: A Principle of the Law of Armed Conflict?', in Mariëlle Matthee, Brigit Toebes, Marcel Brus, eds., *Armed Conflict and International Law: In Search of the Human Face* (The Hague: Asser, 2013), 33–51.

19 ICRC, *Handbook on International Rules Governing Military Operations* (Geneva: ICRC, 2013), 53, Department of Defense, *Law of War Manual* (Washington, DC: DoD, 2016), 50, Ministry of Defence, *Manual of the Law of Armed conflict (JSP 383)* (London: MoD, 2004), 21–23, Chief of Defence Staff, *Joint Doctrine Manual Law of Armed Conflict at the Operational and Tactical Levels* (Ottawa: National Defence Headquarters, 2001), 2–1.

20 Koninklijke Landmacht, *Handleiding Humanitair Oorlogsrecht* (Den Haag: Koninklijke Landmacht, 2005), 30. With some minor differences these principles are

accepted by most Western nations like United States, United Kingdom, Canada and also by organisations such as the ICRC and NATO.

21 Codified in amongst others ICRC, *API*, art. 48: 'The parties to the conflict […] shall direct their operations only against military objectives'.
22 ICRC, *API*, art 51, 5 (2).
23 Ibid., art 51, 1.
24 Ibid., art.52 (2).
25 Perfidy is defined in ICRC, *API*, art. 37 as: 'Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or obliged to accord, protection under the rule of international law applicable in armed conflict, with the intent to betray that confidence'. The article clarifies that 'it is prohibited to kill, injure or capture an adversary by resort to perfidy'. The question that remains, however, is whether perfidy that does not lead to 'kill, injury or capture' is also prohibited.
26 An example is the proportionality rule for attacks. The legal obligation is in the application of this rule. The outcome, the commander's judgement whether or not incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof is excessive in relation to the concrete and direct military advantage, will depend also on moral and operational arguments.
27 Only military advantage is required vs concrete and direct military advantage. The latter is a higher standard.
28 Just as with attacks, chivalry can support the reasonable commander while deliberating proportionality.
29 International Criminal Tribunal for the former Yugoslavia (ICTY), *Final Report to the Prosecutor* (The Hague, ICTY, 2000), par. 50.

References

Bosch, Bart van den, *Oorlog voeren zonder geweld* (Amsterdam: Amsterdam University, 2019), https://dare.uva.nl/search?identifier=8c79d32a-8568-41a2-a4f0-00df37ca6a87.

Chief of Defence Staff, *Joint Doctrine Manual Law of Armed Conflict at the Operational and Tactical Levels* (Ottawa: National Defence Headquarters, 2001), https://www.fichl.org/fileadmin/_migrated/content_uploads/Canadian_LOAC_Manual_2001_English.pdf.

Department of Defense, *Law of War Manual* (Washington, DC: DoD, 2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190=

Dörmann, K., 'Applicability of the Additional Protocols to Computer Network Attacks', in Karin Bystrom, ed., *Proceedings of the International Experts Conference on Computer Network Attacks and the Applicability of International Humanitarian* Law (Stockholm: Swedish National Defence College, 2005).

Gill, T., 'Chivalry: A Principle of the Law of Armed Conflict?', in Mariëlle Matthee, Brigit Toebes, Marcel Brus, eds., *Armed Conflict and International Law: In Search of the Human Face* (The Hague: Asser, 2013), 33–51.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Security, *Transmits Report A/68/98* (New York: UN, 2013).

Henckaert, J.M., and Doswald-Beck, L., *Customary International Humanitarian Law, Volume I: Rules* (Cambridge: Cambridge University Press 2005).

ICRC, *Additional Protocol I to the Geneva Conventions* (Geneva: ICRC, 1977).

ICRC, *Handbook on International Rules Governing Military Operations* (Geneva: ICRC, 2013).

ICTY, *Final Report to the Prosecutor* (The Hague, ICTY, 2000).

Koninklijke Landmacht, *Handleiding Humanitair Oorlogsrecht* (Den Haag: Koninklijke Landmacht, 2005).

Mačák, K., 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law', *Israel Law Review* 48:1 (2015), 55–80.

Ministry of Defence, *Manual of the Law of Armed Conflict (JSP 383)* (London: MoD, 2004),
https://www.gov.uk/government/collections/jsp-383.

NATO, *Brussels Summit Declaration* (Brussels: NATO, 2018),
https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack', *International Review of the Red Cross* 96:893 (2014), 189–206.

Schmitt, M., ed., *Tallinn Manual on the International Law applicable to Cyber Warfare*, (Cambridge: Cambridge University Press 2013).

Schmitt, M., 'Wired Warfare: Computer Network Attack and *jus in bello*', *International review of the Red Cross* 84:846 (2002).

United Nations, *Statute of the International Court of Justice* (San Francisco, CA: United Nations, 1945).

14 Cyber operations and targeting rules

Raïssa van den Essen

Introduction

Cyber operations have become a reality in contemporary armed conflict.[1] NATO member states publicly expressed their need for 'cyberwarfare capabilities' in the mid-2000s, but it wasn't until late 2018 that five such alliance members, the United States, the United Kingdom, Denmark, Estonia, and the Netherlands, announced that they would contribute national cyber forces to NATO missions and operations.[2] Aside from such commitments states including the United States, the United Kingdom and Australia have publicly spoken of their use of offensive cyber capabilities against IS.[3] Former prime minister Malcolm Turnbull of Australia commented on his country's use of cyber capabilities in its operations against IS by stating that

> (…) they are making a real difference in the military conflict and that all offensive cyber activities in support of the Australian Defence Force and our allies are subject to the same rules of engagement which govern the use of our other military capabilities in Iraq and Syria, such as our F-18 Hornets.[4]

While his former point seems undeniable, Turnbull's latter point regarding the manner in which offensive cyber activities are subjected to a certain ruleset has become a topic of discussion among scholars of International Humanitarian Law (IHL). Turnbull's statement may be understood as implying that all offensive cyber activities are subjected to the same ruleset as other, kinetic, military capabilities. As to IHL, this may be the case for cyber operations which are deemed 'attacks' on the basis of their violent (physical) effects, but cyber operations lacking such effects may well fall outside of that ruleset.[5]

Discussion regarding cyber operations lacking physical effects and the manner in which they may be subjected to the targeting rules of Additional Protocol I to the Geneva Conventions of 1949 (API) has evolved around two main topics. These topics are whether such operations can be considered attacks, and whether data in and of itself can be considered a damageable

object.[6] The first question is relevant because targeting rules concern activities that are considered attacks in the sense of art. 49 API, acts of violence in offence or defence. The application of various IHL constraints and conditions, which protect the general population, depends upon an operation constituting such an attack. A consequence of classifying cyber operations lacking physical effects as 'non-attacks' is the inapplicability of such conditions and restraints. The question regarding the status of data as an object is of pertinence because 'civilian objects' are protected under API. If data is not an 'object' it cannot be a civilian object and it cannot be protected as such under API's targeting rules.

In this chapter I contend that the notion of 'damage', while having received less attention, is of equal importance in discussing cyber operations and targeting rules. Damage of physical structures is a common visual representation of the outcome of war, but what does this concept mean in regard to cyber operations lacking physical effects?

This chapter first outlines the discussions regarding the interpretation of IHL's 'attack' and 'object' in the context of cyber operations. Subsequently it considers 'damage', which forms an important element of targeting decisions, in the context of the drafting process of the API. It will be concluded by an appraisal of how different approaches towards the interpretation of attack, objects and damage will influence the understanding of the manner in which targeting rules govern cyber operations.

The interpretation of 'attack', 'object' and 'damage' in cyber operations

May 5, 2019 marked the first time a state publicly described having responded to cyber operations through kinetic force. Escalating violence between Israel and Hamas formed the background against which the Israeli Defence Force (IDF) targeted a building in Gaza, resulting in its partial destruction. What had made this building a military objective, according to the IDF, was its alleged use as a Hamas cyber operatives' headquarters from which attacks against Israel were directed.[7] The operation was explained as having consisted of two parts: the first part was characterised as 'a cyber defensive operation' to neutralise the digital threat; the second part consisted of an airstrike on the building. Various questions have been raised about the legality of this attack, the extent to which it was a 'first of its kind', and the necessity of the kinetic attack after the successful cyber operation. In relation to the subject matter of this chapter the main question regarding this operation concerns its qualification as an attack in the sense of art. 49 API, in the hypothetical case that the airstrike had not occurred.[8]

In June 2019 cyber operations were undertaken against Iran by the United States in response to the oil tanker attacks in the Gulf of Oman earlier that month, and the downing of a US drone on June 20th.[9] While a kinetic response had been considered, a different route was chosen, namely that

of US Cyber Command conducting cyber operations against the Islamic Revolutionary Guard Corps (IRGC) and other targets.[10] In this case a question can be posed as to the nature of such a response had it taken place in the context of an armed conflict between the two States; would it have been regarded as an attack in the sense of art. 49 API? What would the military objective of such an attack consist of, and could the generated effects constitute the type of damage referred to in art. 57 API?

Answers to these hypothetical questions depend upon the interpretation of the notions of attack, object and damage as meant in API. In the cased described earlier the outcome of the cyber operations consisted of functional interference. US Cyber Command stated to have disabled Iranian computer systems controlling its rocket and missile launchers, while the IDF spoke of a successful operation that brought an end to the cyber-attacks by Hamas. Whether these effects are considered enough for the operations to constitute an attack in the sense of art. 49 API depends on whether such effects are considered 'violent'. In the case of Iran, if it was the underlying physical infrastructure that was targeted, the interference in the functionality of that infrastructure could be understood as the damage suffered by an attack while the infrastructure itself would be the military objective. However, if replacing physical parts to regain functionality would not be necessary and the target was of a purely virtual nature, the answer to such questions may be that there was neither an attack nor damage. These different outcomes depend upon the inclusion of data as an object that can be damaged in the interpretation of API's targeting rules.

The following sections describe how our current understanding of attacks, objects and damage yields different answers depending on the interpretation of the relevant rules, and how this, in turn, can influence targeting decisions in the conduct of contemporary warfare.

The changing nature of 'attacks'

The interpretation of attack in the sense of art. 49 API is changing. A notion that in the past signified violent actions, then moved to also encompass actions having violent effects, currently appears to be shifting towards a broader spectrum of effects which includes certain cyber operations. An attack in IHL is defined as an act of violence against the adversary, committed in offense or defence.[11] The definition of the term cyber-attack presented by the Group of Experts (GoE) in the Tallinn Manual 2.0 closely resembles that and reads, 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[12] Acts of violence do not require the release of kinetic force to qualify as such but necessitate violent consequences.[13] Attacks on data, foreseeably resulting in injury, death of persons, or damage or destruction of physical objects, thus qualify as attacks that considered those persons or objects as their 'objects of attack'. [14]

A majority of the GoE was of the opinion that interference in functionality would qualify as an attack if restoration of functionality required the replacement of physical components.[15] Some of the experts considered such interference to already be present if reinstallation of particular data or the operating system was necessary, while others were of the opinion that loss of usability in itself was enough.[16]

The International Committee of the Red Cross (ICRC) noted that regardless of the object being disabled by kinetic or cyber means it would regard operations designed to disable, for example, a computer or computer network as an attack that falls within the scope of IHL.[17] This position is in line with that which was expressed by France in its declaration on International Law Applicable to Operations in Cyberspace.[18] The declaration states that cyber operations may constitute attacks in the sense of art. 49 API if they lead to physical damage or if they render a system inoperative. An attack is also understood to take place if an equal effect is produced to the destruction of computer systems or equipment by alteration or deletion of digital data or digital data flows which render essential services to the functioning of these capacities inactive. In addition, cyber operations causing temporary or reversible effects are considered attacks when intervention is essential through, for example, repairs of the system, replacement of parts or reinstallation of the network to regain the targeted systems functionality.[19]

The foregoing shows that the understanding of the 'act of violence' necessary to constitute an attack in the sense of art. 49 API is changing. Following the interpretation of the GoE the IDF's cyber operation against Hamas' cyber operations would not be an attack unless undoing the effects would necessitate the replacement of physical parts. Following the position of France and the ICRC, however, this operation would have been an attack even without the need for physical replacement of parts. US Cyber Command's operations against Iran, leading to loss of intelligence and necessitating repairs of a critical communication network used by the IRGC, lead to an identical outcome.

Data and the interpretation of 'objects'

Assuming cyber operations lacking physical effects can constitute attacks, the next relevant question concerns which targets are considered legitimate. A short answer would be 'all targets that are military objectives' as civilian objects may not be targeted under IHL. Unfortunately, in the context of cyber operations, that answer does not suffice. To do so it must first become clear what was meant by 'objects' and whether data is encapsulated by that notion.

Art. 52 API establishes that civilian objects are all objects which are not military objectives. Paragraph 2 of this article explains military objectives as objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation offers a definite military advantage. Accordingly,

effective contribution and military advantage are the elements by which an object can be identified as a military objective.[20] Following the Tallinn Manual 2.0, attacks on data resulting in damage or destruction are understood to have had the damaged or destroyed physical object as their object of attack. [21] The majority opinion contended that, based on the ICRC Commentary to art. 52 API, the term object is to be understood as something that is visible and tangible. Consequently, data could not constitute a military objective or a civilian object.[22] Save for some exceptions, the consequence of this interpretation is that an attack on data in and of itself cannot qualify as an attack in the sense of art. 49 API.

The Manual was found to make use of an irrelevant criterion of tangibility, with Droege arguing that it should not make a difference whether a civilian object is made unserviceable due to physical damage or through interference with its operating system.[23] In addition, bypassing data and focussing on the underlying infrastructure was stated to cause practical issues, as data and code are not necessarily tied to a single piece of hardware.[24] Multiple instances of an operating system may be run by a single server, not all of which are tied to the military objective in question.[25] Civilian computer systems unknowingly involved in a botnet could, for example, create a wide range of intangible virtual assets that qualify as legitimate targets.[26]

Both the high level of interdependence between civilian and military infrastructure, and the increasing precision with which parts of a system can be targeted resulted in questions regarding the appropriate scope and the precise level at which the military objective should be defined.[27] The mere fact that data is intangible was challenged as a justification to preclude it from being considered a military objective if the other criteria of art. 52²API were met.[28] Bringing data within the scope of IHL was argued to be in line with an evolutive approach to the interpretation of the military objective. It was also noted that art. 52² API's test to establish whether something is a military objective seems suitable in its application to data but the interpretation of data as a non-object impedes this substantive assessment.[29] Arguments regarding objects' necessary tangibility and visibility in essence intend to impede an interpretation of the term that goes beyond what was intended by API's drafters. However, in doing so the practical realities indicated by the criticism on this position are ignored. The increased societal importance of data as well as the intent of API being a treaty of a long duration makes for compelling arguments in favour of an evolutive approach to its interpretation instead of excluding data as a non-object altogether.

The understanding of damage in IHL and its implications for cyber operations

The discussion on whether data is a protected civilian 'object' is of importance in regard to targeting decisions as its outcome could influence the extent to which civilian data can become part of cyber operations. Likewise,

the understanding of damage will influence the manner in which cyber operations' effects are appraised against targeting rules. IHL differentiates between combatants and civilians.[30] It protects civilian objects against damage and destruction through prohibitions and prescribes precaution to be taken in attack so as to ensure the minimisation of risk for the civilian population and their objects.[31] For the effectiveness of such rules it must be clear what is considered as damage. Whether it is constricted to physical damage or includes non-physical effects has direct consequences for the precautions that must be taken in attack and proportionality assessments in cyber targeting decisions.

Different fields of law use different points of reference to perceive damage. Criminal law protects victims of criminal offences against damage that is both material and immaterial in nature, property, health and safety. Civil and administrative law protect against damage of a material or financial kind.

Within IHL's framework the understanding of damage is based upon different reference points. The first is IHL's objective of protecting civilians and their property against the violent consequences of conflict. This can be found in the principles of IHL, most notably that of distinction, humanity and proportionality. In addition, IHL's objective of regulating the means and methods of warfare forms an important factor in the way damage is purposed in this legal framework.

The meaning of damage in IHL can be summarised as the physical harm that impairs the value, usefulness or normal function of an asset. In addition, it is distinct from destruction in that it covers effects that can theoretically be repaired or reversed as against the irreparable effects of destruction. Damage in this sense has been mostly of a physical nature. Damage of a non-physical nature, but within the domain of IHL, has consisted of contamination of an area or of objects in the aftermath of a chemical, biological or nuclear attack.[32] Physical damage to civilian objects during an attack on a military objective can be lawful, if it is not excessive in light of the expected military advantage.[33] This is an assessment following the rule of proportionality, which specifies that planners and decision makers must refrain from launching attacks that are deemed disproportionate. Art. 57[1] requires constant care to be taken in the conduct of military operations to spare the civilian population and civilian objects.

Paragraph 2 states that planners and decision makers are to do everything feasible to ensure that targeted objects are indeed lawful targets. All feasible precautions should be taken in the choice of means and methods of attack to avoid or minimise incidental loss of civilian life or injury and damage to civilian objects; attacks that are expected to be disproportionate in its collateral consequences should be avoided. In order to fulfil these requirements, it must be clear what is considered as damage in the context of cyber operations. The GoE considered cyber operations to be damaging when there would be foreseeable damage or destruction of physical objects and when loss of functionality would require replacement of physical components.[34]

Jensen reviewed several approaches to determination of damage in cyberspace. He commended an approach in which damage encompasses interruptions in functionality which would require the replacement of parts or the restoration of software systems.[35] It was stated to include the unique aspects of cyber operations while keeping the legal standard easily understandable for commanders in their proportionality assessments by focussing on functionality.[36] This functionality approach differs from that proposed by the majority of the GoE, as it includes restoration of software as well as replacement of physical components. Kilovaty comments on this difference by stating that the approach in the Tallinn Manual misses the point of functionality as a standalone value that is to be protected regardless of physical damage that may or may not be linked to it.[37]

To effectively provide protection against damage it must be clear what is meant by that notion. In regard to cyber operations the question is whether non-physical effects fall within the term's scope. Jensen's functionality approach takes effects into account which interfere with functionality, regardless of the need for physical replacements in order to restore it. Such an approach appears to be in line with the interpretations of France and the ICRC regarding 'attack'.

The following two sections will present considerations concerning the use of the term damage stemming from the drafting phase of API. They concern the differences between 'damage', 'effects' and 'destruction', thereby arguing in favour of further substantive discussion concerning damage in the context of cyber operations.

Damage vs effects

The term damage was the topic of debate when effects of armed conflict on the environment were discussed while drafting API. Points of discussion were the rationale behind using 'effects' instead of 'damage' and the lack of substantive discussion regarding the term damage while perspectives on its interpretation diverged. Art. 35 API prohibits the use of methods or means of warfare which are intended to or may be expected to cause widespread, long-term and severe damage to the natural environment.[38] This article offers protection to the environment itself against intended or expected damage.[39] There are notable differences between the text of this provision and that of a similar provision in the draft Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD) that was the result of the 1975 Conference of the Committee on Disarmament (CCD).[40] The ENMOD mentions environmental modification techniques having widespread, long-term or severe effects.[41] This terminology differed from that of API as the words used there were 'long-term' instead of long-lasting and 'severe effects' instead of severe damage. These differences were explained as long-term denoting a period of months or a season, while long-lasting refers to decades.[42] The difference between

severe effects and severe damage, however, was left largely unexplained. Divergence between the provisions in the draft ENMOD and API was also the consequence of the former being aimed at the effects of geophysical war while the API provision relates to ecological war.[43] This explanation was shared by the US representative to the CCD who stated that art. 35 API's objective was to protect the natural environment against damage which could be inflicted upon it by any weapon, whereas the ENMOD intended to prevent the use of environmental modification techniques as a weapon.[44] The use of the term 'effects' was clarified by the representatives of the Soviet Union as making it possible to include the prohibition of environmental modification techniques not having a hostile character and not designed to cause destruction, damage or injury but which could lead to unwanted effects nonetheless.[45]

The drafting history of art. 35 API shows that discussions such as those relating to the ENMOD Convention on the actual meaning of damage are absent. While the elements of time, duration and scope of the affected area were extensively discussed, the use and meaning of the term damage was not.[46] However, the Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts (Official Records) mention that an alternative formula of causing damage had been formulated, namely; 'to disturb the stability of the ecosystem'.[47] This formula was rejected but it shows that while views may have been convergent regarding its adoption, there were different ideas regarding the threshold by which 'damage' was to be understood.

Furthermore, the Working Group reporting to Committee III stated that it recognised that environmental change or disturbances of the ecosystem might be on a very low scale, citing cut down or destroyed trees due to artillery fire as an example, and stating that such short-term damage was not the subject of the prohibition.[48] The use of 'change and disturbances' is relevant as it may be understood as an indication of the Working Group recognising that such effects, while not meeting the required threshold, were to be understood as a low-level form of damage. Terms were deliberately chosen by the drafters of the ENMOD to extend its scope and include 'unwanted effects'. While the term 'damage' was not substantively discussed, it was understood by way of a threshold that had to be met before consequences would qualify as the type of damage against which API protected. In discussing effects of cyber operations and API's concept of damage, a threshold which is solely linked to physicality does not seem adequate in light of IHL's aim of protecting civilians against the dangers of hostilities and the current reality of data-dependency.

Damage vs destruction

The following section shows that the original intent of API's drafters was for 'damage' and 'destruction' to designate different thresholds of protection. As to cyber operations such an indication can be of use in interpreting

'damage' in a manner that is in line with the original intent of API's drafters. Art. 51 API offers general protection to the civilian population and individual civilians against dangers arising from military operations and prohibits making them the object of attack, or be subjected to acts or threats of violence that are intended to spread terror among them.[49] The term damage in this subsection denotes the detrimental effects of a violent act. This can be inferred from the Commentary to this article which states that the types of attacks considered here are area bombardments and those causing excessive effects in relation to the concrete and direct military advantage anticipated.[50] The original text by the ICRC diverged from the final text in that it specifically prohibited the 'destruction' of civilian objects.[51] Where this was originally 'incidental loss and destruction', the final text added 'injury' and replaced 'destruction' by 'damage'. The Official Records do not mention how this change in wording came to be, but the replacement of 'destruction' by 'damage', as well as the insertion of 'injury', appears to imply an expansion of the provision's scope and a lowering of its threshold. During discussions relating to the draft version of art. 51 API the difference in wording was referred to by the representative of Sweden who commented that the text of draft art. 50 (later: art. 57 API) was preferable to that of draft art. 46 (later: art. 51 API) as art. 46 did not mention the 'damage' that the civilian population might suffer.[52] Draft art. 46 indeed did not mention damage but spoke of 'causing destruction of civilian objects to an extent that is disproportionate to the direct and substantial military advantage expected'.[53] The change in wording, moving from a prohibition of destruction to a prohibition of damage, may be indicative of a threshold change and of the different connotations these notions have in IHL's framework. Further analysis of such an indication is warranted, in general, and in relation to cyber operations. Clarity regarding the meaning and scope of this notion is a necessary element of interpreting API's targeting rules in contemporary armed conflict.

Conclusion

The addition of cyber capabilities to states' offensive and defensive options during conflict has changed the character of war. API originates from a period in which cyber operations and their effects were not yet part of the conduct of hostilities, and in which society's future dependence on computer networks and systems was unforeseen. The references made by API to attacks, objects and damage could therefore be relegated to exclude effects of cyber operations that lack any physicality. However, they could also be interpreted using a more evolutive approach which includes interferences in functionality as the damaging consequences of an attack that targeted data. International legal discussion on this topic has brought forth different approaches for the interpretation of these notions. Further deliberation as well as state practice will eventually lead to an understanding of the manner in which cyber operations are, or are not, governed by the targeting rules of API.

Notes

1 ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts', *ICRC Position Paper*, November 2019, 2.
2 Max Smeets, 'NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis', *2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2019, 7.
3 Ibid., 2.
4 Rohan Pearce, 'Government Reveals Offensive Cyber Operations against IS', *Computer World*, 23 November 2016, https://www.computerworld.com/article/3480555/government-reveals-offensive-cyber-operations-against-is.html
5 Ibid.
6 Michael Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations', *International Review of the Red Cross* 101:910 (2019), 3–4.
7 Lily Hay Newman, 'What Israel's Strike on Hamas Hackers Means for Cyberwar', *Wired*, 6 May 2019, https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar.
8 Hay Newman, 'Israel's Strike', Robert Chesney, 'Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility', *Lawfare*, 6 May 2019, https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.
9 Julian E. Barnes, 'U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say', *The New York Times*, 28 August 2019.
10 Robert Chesney, 'A Cyber Command Operational Update: Clarifying the June 2019 Iran Operation', *Lawfare*, 3 September 2019, https://www.lawfareblog.com/cyber-command-operational-update-clarifying-june-2019-iran-operation.
11 ICRC, *Additional Protocol I to the Geneva Conventions* (*API*) (Geneva: ICRC, 1977), Art. 49.
12 Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), Rule 92.
13 Ibid., par. 3.
14 Tallinn Manual 2013, Commentary to Rule 30, par. 6.
15 Schmitt, *Tallinn Manual 2.0*, Rule 92 par. 10.
16 Ibid., par. 11, 12.
17 Laurent Gisel and Lukasz Olejnik, *The Potential Human Cost of Cyber Operations* (Geneva: ICRC, 2019).
18 Ministère des Armées, *Droit international appliqué aux opérations dans le cyberspace* (Paris: Ministère de Armées, 2019), par. 2.2.1.
19 Ibid.
20 Claude Pilloud, Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann, eds., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: International Committee of the Red Cross, Martinus Nijhoff Publishers, 1987), par. 2018.
21 Schmitt, *Tallinn Manual 2.0*, Rule 92, par. 4.
22 Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law', *Israel Law Review* 48:1 (2015), 59.
23 Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians', *International Review of the Red Cross* 94:886 (2012), 558.
24 Heather A. Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives', *Israel Law Review* 48:1 (2015), 40.
25 Ibid.
26 Robin Geiß and Henning Lahmann, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space', *Israel Law Review* 45:3 (2012), 384.
27 Harrison Dinniss, 'The Nature of Objects', 50–51.

28 Ibid., 54.
29 Ibid., 65, Mačák, 'Military Objectives 2.0', 70–71.
30 And other non-combatants.
31 ICRC, *API*, Art. 57.
32 ICRC, *API*, Art. 55.
33 A.R. Thomas, and James C. Duncan, eds., *Annotated Supplement to the Commander's Handbook on the Law of Naval Operations* (Newport, RI: Naval War College, 1999), 404–405.
34 Schmitt, *Tallinn Manual 2.0*, Rule 92 par. 6.
35 Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack', *International Law Studies* 89 (2013), 205–206.
36 Ibid., 207.
37 Ido Kilovaty, 'Virtual Violence-Disruptive Cyberspace Operations as Attacks under International Humanitarian Law', *Michigan Telecommunications and Technology Law Review* 23 (2016), 126.
38 ICRC, *API*, Art. 35.
39 Pilloud, Sandoz, Swinarski, Zimmermann, Commentary, par. 1440.
40 Ibid., par. 1448. This would become the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD). Paragraph 1 reads: 'Each State Party to this Convention undertakes not to engage in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party'.
41 Ibid., par. 1448.
42 Ibid., par. 1452.
43 Ibid., par. 1461–1462.
44 United Nations General Assembly, *Report of the Conference of the Committee on Disarmament* (New York: United Nations, 1976), 72.
45 Ibid., 66.
46 *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts* (Geneva, 1978), 268.
47 Ibid.
48 Ibid., 359. Committee III of the Geneva Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflict of 1977.
49 ICRC, *API*, Art. 51 (1) (2).
50 Pilloud, e.a., *Commentary*.
51 ICRC, *Draft additional Protocol I to the Geneva Conventions* (Geneva: ICRC, 1973), Art. 46.
52 *Official Records*, XIV, 191.
53 ICRC, *Draft API*, Art. 46(3) sub (b) read: '(it is prohibited…) to launch attacks which may be expected to entail incidental losses among the civilian population and cause the destruction of civilian objects to an extent disproportionate to the direct and substantial military advantage anticipated'.

References

Barnes. J.E., 'U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say' *The New York Times*, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html 28 August 2019 (28 August 2019).

Chesney, R., 'A Cyber Command Operational Update: Clarifying the June 2019 Iran Operation' *Lawfare*, https://www.lawfareblog.com/cyber-command-operational-update-clarifying-june-2019-iran-operation. (03 September 2019).

Chesney, R., 'Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility', *Lawfare*, https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility. (06 May 2019).

Corn, Geoffrey S., ed., *The War on Terror and the Laws of War: A Military Perspective* (New York: Oxford University Press, 2015).

Dinstein, Y., 'Legitimate Military Objective under the Current Jus in Bello', *International Law Studies* 78*, Legal and Ethical Lessons of NATO's Kosovo Campaign*, (2002), Andru E. Wall, ed. (Newport, RI: US Naval War College's International Law Studies, 2002), 139–172.

Droege, Cordula, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians', *International Review of the Red Cross* 94:886 (2012), 533–578.

Ducheine, Paul A. L., Schmitt, Michael N., Osinga, Frans P.B., eds. *Targeting: The Challenges of Modern Warfare* (The Hague: Asser, 2016).

Fortson, Larry W., *Towards the Development of a Defensive Cyber Damage and Mission Impact Methodology* (Dayton, Air Force Institute of Technology, 2007).

Geiß, Robin, and Lahmann, Henning, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space', *Israel Law Review* 45:3 (2012), 381–399.

Gisel, Laurent, and Olejnik, Lukasz, 'The potential human cost of cyber operations' (Geneva: ICRC, 2019).

Harrison Dinniss, Heather A, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives', *Israel Law Review* 48:1 (2015): 39–54.

Hay Newman, Lily, 'What Israel's Strike on Hamas Hackers Means For Cyberwar', *Wired*, 6 May 2019, https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar.

ICRC, *Additional Protocol I to the Geneva Conventions* (Geneva: ICRC, 1977).

ICRC, *Draft additional Protocol I to the Geneva Conventions* (Geneva: ICRC, 1973).

ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts', *ICRC Position Paper*, November 2019.

Jensen, Eric Talbot, 'Cyber Attacks: Proportionality and Precautions in Attack', *International Law Studies* 89 (2013), 198–217.

Kilovaty, Ido, 'Virtual Violence-Disruptive Cyberspace Operations as Attacks under International Humanitarian Law', *Michigan Telecommunications. & Technology Law Review* 23 (2016), 113–147.

Mačák, K., 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law', *Israel Law Review* 48:1 (2015), 55–80.

Ministère des Armées, *Droit international appliqué aux opérations dans le cyberspace* (Paris: Ministère de Armées, 2019).

Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts (Geneva, 1978).

Pascucci, Peter, 'Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution', *Minnesota. Journal of International Law* 26 (2017), 419–461.

Pilloud, Claude, Sandoz, Yves, Swinarski, Christophe, Bruno Zimmermann, and International Committee of the Red Cross, eds. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: International Committee of the Red Cross, Martinus Nijhoff Publishers, 1987).

Rabkin, Jeremy A., and Rabkin, Ariel, 'To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict', in *Emerging Threats Essays* (Stanford, CA: Stanford University, 2012), http://www.hoover.org/sites/default/files/uploads/inline/docs/EmergingThreats_Rabkin.pdf.

Rohan Pearce, 'Government reveals offensive cyber operations against IS', *Computer World* 23 November 2016, https://www.computerworld.com/article/3480555/government-reveals-offensive-cyber- operations-against-is.html.

Roscini, Marco, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014).

Schmitt, Michael N., ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

Schmitt, Michael N., 'The Notion of "Objects" during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision', *Israel Law Review* 48:1 (2015), 81–109.

Schmitt, Michael N., 'Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations', *International Review of the Red Cross* 101:910 (2019), 1–23.

Smeets, Max, 'NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis', *2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2019, 1–15.

United Nations General Assembly, *Report of the Conference of the Committee on Disarmament* (New York: United Nations, 1976).

15 Contemporary urban warfare

Does international humanitarian law offer solutions?

Jeroen van den Boogaard

Introduction

On 27 March 2019, the *Jerusalem Post* reported that Hamas blamed the Palestinian Authority for helping the Israel Defense Forces (IDF) to conduct attacks in Gaza. According to the report, Hamas said that calling and texting civilians that their homes were under imminent attack would constitute assistance to the enemy. Reportedly, Hamas spokesman Sami Abu Zuhri said that the alleged phone calls:

> reflect the filthy role the Palestinian Authority [PA] played in collaborating with the occupation in the war against our people (…) Palestinian Authority security forces were behind phone calls to Palestinians in the Gaza Strip to leave their homes before they were hit by Israeli airstrikes. The source told the Hamas-affiliated Shehab news agency that the PA's General Intelligence Force – headed by Majed Faraj – was behind some of the phone calls made to residents and institutions during Monday's Israeli military strikes, which came in response to the launching of a rocket from the Gaza Strip to the Kfar Saba region….[1]

At first appearance, this seems to be a typical example of 'lawfare': one party to an armed conflict discrediting its opponent by misusing the law, because Hamas frames the phone calls as an illegal act, namely assistance of the enemy.[2] A second reading however suggests that the Palestinian Authority was probably complying with the applicable law and its action was aimed at saving civilian lives. If the Palestinian Authority was informed by the IDF that the air strikes were imminent, this seems to comply with the IDF's legal obligation to do all in its power to warn the authorities, and the obligation of the Palestinian Authority to take necessary precautions to protect the civilian population. These obligations arise from the legal framework that applies specifically to armed conflict: international humanitarian law (IHL).

This chapter aims to explain which solutions IHL offers to enhance the protection of the civilian population in contemporary urban warfare. Armed conflicts during the last decade brought renewed emphasis on urban

operations in Gaza, Syria, Iraq and Yemen. The armed conflicts between states and non-state actors, for example the operations against Islamic State (IS) in Iraq and Syria and those between rebel forces and the Syrian government in Aleppo, Homs and other cities mark the return of a classic method of warfare: sieges.[3] One by one, cities and towns in Iraq and Syria were encircled and subsequently recaptured from IS or other violent non-state actors. An integral part of siege warfare is close range urban warfare, often supported by extensive use of artillery and air-delivered (precision) munitions. This method of warfare has left many villages, towns and cities in both Syria and Iraq almost completely destroyed. Research conducted by the International Committee of the Red Cross (ICRC) suggests that hostilities in urban areas in Iraq and Syria is eight times more deadly for civilians than warfare in other areas.[4] Similarly, since the escalation of the armed conflict in Yemen since 2014, artillery and air strikes killed scores of civilians and the 'blockade, siege-like tactics, attacks impacting objects essential to the survival of the population and impediments to the delivery of aid deprive the population of necessary items amidst the unprecedented humanitarian crisis'.[5]

This chapter aims to identify which legal obligations offer solutions for the protection of the civilian population during contemporary urban warfare. In this context, the legal framework applicable to urban warfare is first set out. Subsequently, the framework's rules concerning precautions in attack are explained, particularly those with regard to warnings. Also, the delicate balance between the feasibility of the precautions in attack in the context of urban warfare is addressed, as well as the dangers of instrumentalisation of IHL obligations as 'lawfare', since these two issues impact on how precautions may be successful in reducing the impact of the conduct of war at present and in the near future on the civilian population. The example of the phone calls allegedly made by the Palestinian Authority to civilians in Gaza is revisited in this light in the conclusion.

The legal framework to urban warfare: IHL

IHL aims to regulate the conduct of hostilities by restricting means and methods of warfare and by providing rules protecting those who do not or no longer participate in hostilities. It applies whenever states use armed force against each other and when hostilities of a certain intensity arise between a state and a violent non-state actor (VNSA) or among VNSAs.[6] IHL consists of a rich variety of treaty rules as well as rules of customary international law, based on a careful balance between what is militarily necessary on the one hand and the principle of humanity on the other hand. IHL applies equally to both states and other parties to the conflict and to warfare in all dimensions: on the ground, in and from the air, to naval warfare that affects the situation on land and to cyber operations.

When it comes to the conduct of hostilities, including in urban warfare, the relevant IHL rules are based on the principles of distinction, proportionality and precautions.[7] These rules are predominantly codified in the 1977 Additional Protocol I to the Geneva Conventions (API) and for the most part also recognised as customary rules. In short, that means that they apply in any type of armed conflict and to all parties involved.

Distinction requires parties to the conflict to direct the fight exclusively towards their opponents. Thus, objects may only be attacked if they constitute a lawful military objective such as the enemy's fighting positions, weapons systems or soldiers. Objects such as houses, schools or religious objects are protected as civilian objects, but may lose that protection if they are used for military purposes. Military medical personnel, wounded and sick soldiers, detained persons and civilians are protected from direct attack as they take no part in the hostilities. However, in contemporary urban warfare, it is tremendously difficult to distinguish between military objectives and the forces of the enemy on the one hand and civilians and civilian objects on the other hand, due to their close proximity in the urban setting.

Proportionality, as a final check before an attack may be launched, dictates that a planned attack may proceed only where the expected civilian harm may be expected not to be excessive in relation to the anticipated direct military advantage. Thus, the presence of a single civilian in an important military installation may not preclude a lawful attack on that target, even when it is anticipated that the civilian will most likely be killed in the attack. The IHL proportionality rule thus acknowledges that civilians may be affected by attacks against military objectives, but sets a limit to this collateral damage by relating it to the expected military advantage. In practice, applying the proportionality rule is a complicated matter in any situation where it is not clear-cut that the balance between the military advantage and the collateral damage tilts to one side or the other. Contemporary urban environments may make it even more difficult to establish on what side of the equation persons or objects must be included.

From these three, the IHL rules relating to precautions most significantly provide solutions for the protection of the civilian population in the context of urban warfare, because the precautionary obligations aim to avoid or minimise civilian casualties and damage to civilian objects through a series of practical steps, as is illustrated in the following section.[8]

IHL solutions for urban warfare: precautionary measures

IHL provides for obligations with regard to precautions for both defenders and attackers. Whereas normally the rules apply to any military operation and to the specific situation of attack, whether in offence or defence, some rules are designed particularly for defenders. It is for example their duty to separate military objectives from the civilian population and to remove civilians from the vicinity of military objectives, to the maximum extent

feasible.[9] How far the civilians must be removed from military objectives is not prescribed, but this may be understood as 'a point where the defending party would no longer expect civilians to suffer harm as a result of friendly or hostile fire directed against that particular military objective'.[10] It should be noted that the defenders must comply with these obligations only to the extent they are in a position to do so. The ICRC commentary to this obligation explains that there is, first, a territorial exception. The obligations are restricted to 'measures which every Power must take in its own territory in favour of its nationals, or in territory under its control'.[11] In order to maximise the protection awarded by this rule, it should already be taken into account in peacetime, because it seems impossible to remove fortified positions and military headquarters and barracks from their location after the armed conflict begins.[12]

For the precautionary measures with regard to attackers, any military operation must comply with the general obligation to take active measures to protect the civilian population. This is the overarching obligation to take constant care to spare the civilian population, civilians and civilian objects.[13] That means in practice that in the planning of an attack, the protection of civilians must be one of the considerations, in addition to other ones, such as how to maximise the effect on the enemy's military capacities. Furthermore, there is a list of more specific precautions that must be taken with respect to the specific situation of attacks.[14]

The first of these is the obligation to ensure that the target of the attack is actually a military objective.[15] This relates back to the rules with regard to distinction, which provide slightly different rules for identifying objects and persons as military objectives.[16] It must be noted that in cases where it is not completely clear whether a certain person is a civilian, it must be assumed that the person is protected from direct attack. As Gillard notes: '[t]his presumption of protected status is the starting point, but the required degree of certainty that an intended target is indeed a military objective is unclear'.[17] Thus, this rule requires that when the time has come to launch an attack against a target, it is not enough that the object was added to a list of military objectives a couple of weeks ago. It needs to be assessed that the object still qualifies as such. For example, if based on two week old information that a house was used by a VNSA for planning military operations, additional information is required to check whether that is still the case.

The second on the list is the obligation to choose, if feasible, that type of attack, or weapon, or munition, that avoids, or at least minimises, incidental loss of civilian life, injury to civilians or damage to civilian objects. This type of precaution could mean that the timing of an attack is adjusted to a moment where no civilians may be expected to be present on the location of the planned attack, or that the calibre, range or fuse of the used munition is limited to the extent that nearby civilian structures may be expected to remain untouched by its impact. Another example may be 'pinpoint attacks' such as the IDF attack killing Hamas leader Ahmed Jabari and his

bodyguard while driving in a car through a narrow street in Gaza City in 2012.[18] For operations in urban areas, it is especially important that care is taken with regard to the use of certain weapons systems. For example, it would seem that the use of explosive area weapons would in some situations be less suitable for the urban environment and could have severe impact on essential drinking water services.[19] This precaution is crucial because it requires the attacker, if feasible, to tweak the possible modes of attack to a point where the protection of the civilian population is optimised in view of the military advantage sought in the planned attack.

There are four more precautions listed: the IHL proportionality rule; the provision that dictates that the precautions must be carried out not only before but also, where feasible, during the attack; the rule that if two military objectives provide an equal military advantage, the one expected to cause the least collateral damage must be chosen as the target; and finally the obligation to warn the civilian population.

The obligation to warn the civilian population is specifically relevant in relation to the situation in Gaza as mentioned in the introduction of this chapter. The rule says that 'effective warning shall be given of attacks which may affect the civilian population, unless circumstances do not permit'.[20] This last part means that the parties do not have an obligation to warn in cases where the element of surprise is crucial to an attack, or when the safety of the attacking forces would be jeopardised by the warning. Obviously, there is no duty to warn the opponent; instead the warning must be aimed at the civilian population. This makes it more practical in case of attacks against objects, rather than persons. In practice, it can be done on close range by using a megaphone or by loudspeakers. On a longer range, warnings may be conveyed by radio broadcasts, by dropping leaflets, by telephone calls or text messages or any other means, as long as it is effective. In relation to the situation in Gaza, it seems that the IDF warned the Palestinian Authority, who, in turn, warned the civilians by calling and texting them. The IDF has developed an extensive system of warning the civilian population, which is not limited to telephone messages but even includes warnings through the launch of small-explosives on the roofs of a military objective, making the message evident that an attack is imminent and civilians need to leave the location immediately.[21]

The duty of attacking forces to take precautionary measures is not limited to those enumerated specifically in the articles on that topic in API.[22] Many other IHL obligations play a direct or indirect role in the protection of civilians through precautionary measures.[23] An example is the prohibition to use starvation of the civilian population as a method of warfare as well as the duty of the parties to the conflict to allow impartial humanitarian relief actions to provide the civilian population with food and other supplies essential to their survival. [24] Another example is the obligation of the attacking party to allow the civilian population to leave the area of hostilities. This is certainly a positive development from the legal restraints on

siege warfare as it was understood before 1899, when it was 'not uncommon (…) that civilians were prevented from exiting a besieged area in order to maximise pressure on the defending commander'.[25] Nowadays, even though there may be no explicit prohibition to disallow civilians to flee from an area of hostilities, IHL stipulates evacuation as an exception to the prohibition of deportation of the civilian population.[26] We have seen this for example at the last major stronghold of IS near the Syrian town of Baghouz in March 2019, after the encirclement of IS was complete. IS was trapped on a small strip of land between the river Euphrates, Syrian Democratic Forces (SDF) and other forces on the other bank of the river. The attacking forces repeatedly halted their operations in order to allow civilians, mostly women and children, to be evacuated from the area, as well as offering IS fighters an opportunity to surrender.[27]

> Examples of indirect precautionary obligations are those concerning the duty to instruct and train military forces in the rules and principles of IHL and perhaps also the duty to include military lawyers in the armed forces.[28] Precautionary measures are also taken above and beyond those provided for by the law. Measures outside the realm of the law include restrictions motivated by political motivations, as included in rules of engagement, or as a result of procedures that military forces have put into place in order to harmonise targeting decisions. [29]

Nonetheless, a host of reasons remains why the damage in the recaptured cities in Iraq and Syria was so extensive. Most importantly, IS had situated their positions inside the cities, rather than in the area around the cities, and the fighting took place amongst the civilian population. This may be assumed to be a direct violation of the duty to take precautionary measures against the effects of the hostilities. Since recapturing these cities from IS constituted the crucial military advantage in this war, it followed that the main battlefields were in the cities. A similar situation occurred in the Syrian cities that were recaptured from rebel forces by Syrian government forces. However, in the old towns of Iraq and Syria, such as Mosul or Aleppo, streets typically were too narrow for manoeuvre warfare; thus house-to-house warfare supported by close air support was needed to clear the area street by street and house by house.[30] For IS specifically is the group that often used powerful car bombs against the approaching troops. Thus, some of the damage in Mosul was the result of violations of the law by IS, using civilians as human shields, or by sending suicide bombers along with fleeing civilians. These suicide bombers would detonate their bomb vests as soon as they reached the opponents forces, killing both them and civilians fleeing for safety.[31] This endangered the lives of the civilians not only directly but also indirectly, as it made Iraqi troops suspicious towards fleeing civilians. Also, the IS positions often included

underground tunnels; thus attacking these positions required large explosive charges. Furthermore, sometimes there were weapons malfunctions or unexpectedly massive secondary explosions occurred when weapons caches were hit or defensive positions on buildings where explosives were planted.[32]

It is clear that a war without civilian casualties does not exist when an opponent is entrenched within urban areas. IHL does not require parties to the conflict to avoid any civilian loss or damage. Instead, precautions must be taken, to the extent feasible.

Urban warfare and feasibility: a delicate balance

As mentioned earlier, the term 'feasibility' is an important component of the precautionary obligations.[33] 'Feasibility' may be understood as slightly more restrictive than the term 'reasonable'.[34] It means that the parties to a conflict cannot 'be required to do the impossible'. Rather, it has been defined as 'that which is practicable or practically possible, taking into account all the circumstances ruling at the time, including humanitarian and military considerations'.[35] In the context of urban warfare this is problematic because military operations and civilians are usually closely co-located. Nonetheless, it is important to note that an attack, or a way of defending a location, can always be executed in multiple different ways and do not always need to be carried out right away, even when this would be more efficient or convenient. For example, dropping a large bomb on a location where multiple military objectives are located may be prohibited if some civilians may be assumed to be present and it is possible to use multiple smaller bombs. But if these types of weapons are unavailable, and it may just be that the air assets present at the scene have already dropped smaller munitions elsewhere, then this precautionary measure is not feasible. It then depends on the outcome of the proportionality analysis whether the attack may proceed or not.

With regard to warning civilians, this is an obligation that is limited by the phrase 'unless circumstances do not permit'. That means that if it may be expected that warning the civilian population will lead to the failure of the attack, warning the civilian population is not feasible. Thus, if the element of surprise is expected to be crucial, this means that the civilian population cannot be warned.

The term feasibility is basically the assurance that military and operational considerations may be taken into account when military operations are underway, and the restraints perceived by the rules of IHL are not unrealistically focussed on the humanitarian side of the coin. This is a delicate balance. Ignoring either side of the coin leads to unacceptable results either in terms of civilian casualties and collateral damage or losses among the own forces. Both factors may incite escalation of the conflict by either party to the conflict and lead to disregard for the law.

Precautions and lawfare

It may be concluded that IHL provides an adequate set of considerations for the protection of the civilian populations against the dangers of contemporary urban warfare. At first sight, concluding that these are 'solutions' seems perhaps incommensurate with the actual civilian casualties and damage to civilian objects in many cities which were retaken from IS in the past years.[36] But the IHL rules provide for explicit obligations and prohibitions to take the protection of the civilian into account in urban operations. Ignoring the law inevitably leads to an increase of civilian suffering. It is true that the implementation of these rules in practice may be improved. But contemporary battlefield practice also proves that IHL is successful in protecting civilians. For example, even though the destruction in Mosul would make one think otherwise, many attacks were cancelled based on precautionary measures. However, these stories are typically not featured by the media.

To refer back to the situation in Gaza, it would seem that framing phone calls that warn civilians to run for safety against incoming bombs as 'assistance to the enemy' is an irresponsible act which decreases the incentive of the parties to a conflict to adhere to the law.[37] The facts do not prove whether Hamas would have welcomed civilian casualties as a useful component of their information operations, blaming and shaming the IDF for causing suffering to the Palestinian civilians, in order to gather support from allies. A Hamas press release as reported by the *Jerusalem Post* could be labelled as a clear example of what is often referred to as 'lawfare'.[38] If lawfare is understood as the 'use of law, or exploitation of aspects of a legal system, to achieve tactical or strategic advantages in the context of conflict' (see also the next chapter), the Hamas press release may then be understood as the misuse of the law to publicly discredit its opponent.[39] However, the concept of lawfare has the potential to blur the proper application of the law. Sometimes it may even be argued that lawfare is used as an excuse to circumvent the equal application of the law of armed conflict, to the detriment of the protection of the civilian population. As a result, the use of the concept of lawfare may lead to an escalation of violations of the law. In this case, instead of shaming the Palestinian Authority and the IDF for adhering to their legal obligation to warn the civilian population, the news article should at least have noted that far more than Hamas propaganda this is an example where IHL is making the difference for one of the purposes for which it was designed: the protection of the civilian population. Thus, there is no place for lawfare in armed conflict. Using situations in which the law was clearly followed as an instrument to discredit the opponent must be avoided in order to protect the integrity of the law.

Concluding remarks

The conduct of war in urban areas is difficult and extremely dangerous for the civilian population because of the co-location of the enemy. Feasible

precautions in attack, including the duty to warn the civilian population, serve to balance the necessities of battle with the obligation to protect the civilian population. Misusing the law for other purposes such as was done by Hamas may seem advantageous to their cause at first sight, discrediting both the Palestinian Authority and Israeli forces. On the long run, however, violations of the law may have the result of complete escalation of the conflict, precluding chances for sustainable peace and must therefore be avoided. Adherence to and implementation of the rules of IHL during the conduct of war are crucial, even when facing an opponent who clearly does not. This is also true because violations of the opponent do not change the own obligation to follow the rules and commanders may be held criminally responsible for their own acts and those of their subordinates. Furthermore, adherence to the rules is the hallmark of effective forces: raping and looting forces lose discipline and become a liability. Lastly, from an operational point of view, treating the opponent and the local population well is likely to increase the protection of the own forces and also induce the willingness of the opponent to surrender rather than fighting until the last man.

As urbanisation will increase further, it may be expected that urban warfare is here to stay.[40] Consequently, troops conducting hostilities at present and in the near future must develop their tactics and procedures to include considerations for protecting the civilian populations in accordance with their precautionary obligations. This may result in challenges to gain military advantage in tactical situations, but it is crucial for strategic purposes because legitimacy in conducting hostilities is ultimately a force-multiplier. Possible lawfare strategies of opponents must thus be countered with strict adherence to the law paired with communication strategies stressing the need to adhere to the law and how that protects the civilian population. The solution to the opponents' lawfare tactics is thus fully ingrained in the obligation to take precautionary measures.

Notes

1 Khaled Abu Toameh, 'Hamas Says PA Helped Israel Attack Gaza', Jerusalem Post, 27 March 2019.
2 See Charles J. Dunlap, 'Introduction to the Concept of Lawfare', National Security Law, J. Norton Moore, G.B. Robert, and R.F. Turner, eds. (Durham: Carolina Academic Press, 2015), 823–838.
3 See also Emanuelle-Chiara Gillard, 'Sieges, the Law and Protecting Civilians', Chatham House Briefing, June 2019.
4 ICRC, 'New Research Shows Urban Warfare 8 Times More Deadly for Civilians in Syria and Iraq', News Release, 1 October 2018.
5 See Group of Experts to the United Nations Human Rights Council, 'Situation of Human Rights in Yemen, Including Violations and Abuses since September 2014', 9 September 2019, A/HRC/42/CRP.1.
6 Generally: International Criminal Tribunal for the former Yugoslavia (ICTY), Prosecutor vs. Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, Appeals Chamber, 2 October 1995, par. 70.

7 See respectively ICRC, Additional Protocol I to the Geneva Conventions (API) (Geneva: ICRC, 1977), articles 48, 51 and customary law rules 1 and 7. See Jeanne Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, Volume I: Rules (Cambridge: Cambridge University Press, 2005), 3-8, 25-29, ICRC, API, articles 51(5)(b), 57 (2)(a)(iii), 57 (2)(b) and customary rule 14. See Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 46-50, ICRC, API, articles 57, 58 and customary rules 15–24. Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 51–76.
8 Jeroen C. van den Boogaard, and Arjen Vermeer, 'Precautions in attack and Urban and Siege Warfare', Yearbook of International Humanitarian Law 20 (2019), 194.
9 ICRC, API, article 58 and customary rules 22–24. See Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 68–76. See also generally Eric T. Jensen, 'Precautions against the Effects of Attacks in Urban Areas', International Review of the Red Cross 98:901 (2016), 147–175 and Aurel Sari, 'Urban Warfare: The Obligations of Defenders', Joint Blog Series, 28 January 2019, https://blogs.icrc.org/law-and-policy/2019/01/28/joint-blog-series-urban-warfare-the-obligations-of-defenders/.
10 Sari, 'Urban Warfare'.
11 Yves Sandoz, Christophe Swinarski, and Bruno Zimmerman, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Geneva: International Committee of the Red Cross, 1987), 692.
12 Ibid.
13 ICRC, API, article 57(1) and the slightly broader customary rule 15. See Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 51–55.
14 ICRC, API, article 57(2), (3) and customary rules 16–21. See Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 55–67.
15 ICRC, API, article 57(2)(a)(i) and customary rule 16. See Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 55–56.
16 For the definition of a military objective where it concerns objects, see ICRC, API, article 52(2). For persons, see for example article 51(2) and (3).
17 Gillard, 'Sieges', 6.
18 See for example David Gritten, 'Obituary: Ahmed Jabari, Hamas Commander', BBC News, 14 November 2012, https://www.bbc.com/news/world-middle-east-20328270. Footage of the attack is available at https://www.youtube.com/watch?v=P6U2ZQ0EhN4&list=ULhFp0Efv5lnI&index=559
19 See for example M. Zeitoun and M. Talhami, 'The Impact of Explosive Weapons on Urban Services: Direct and Reverberating Effects across Space and Time', International Review of the Red Cross, 98:901 (2016), 53–70, referring to drinking water systems.
20 ICRC, API, article 57 (2)(c) and customary rule 20. See Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 62–65.
21 See also Jeroen van den Boogaard, 'Knock on the Roof, Legitimate Warning or Method of Warfare?' Yearbook of International Humanitarian Law 19 (2016), 183–209.
22 For the precautions against the effects of attacks, this is specifically mentioned in ICRC, API, article 58 (c): '[The Parties to the conflict shall, to the maximum extent feasible … take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations'. For precautions in attack, a similar conclusion may be inferred from the general obligation that '[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects'. See ibid., article 57 (1).

23 Geoffrey S. Corn, 'War, Law, and the Oft Overlooked Value of Process as a Precautionary Measure', Pepperdine Law Review 42:3 (2014), 419–466, available at: https://digitalcommons.pepperdine.edu/plr/vol42/iss3/2
24 ICRC, API, article 54 (1) API and customary rule 53. See also Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 186–189, ICRC, API, article 70.
25 Nuremberg Military Tribunal under Control Council Law No 10, United States of America v Wilhelm von Leeb and others, Judgment, 27 October 1948, para 562. The codification of the rules for the conduct of hostilities in a treaty roughly started in 1899 with the adoption of the Hague Conventions, although there were a few predecessors such as the 1863 Lieber Code and the 1868 St. Petersburg Declaration.
26 ICRC, Fourth Geneva Convention (Geneva: ICRC, 1949), article 49, ICRC, API, article 85(4)(a) API and customary rule 129. See Henckaerts and Doswald-Beck, Customary International Humanitarian Law, 457–462. See also Laurie R. Blank, 'Sieges, Evacuation and Urban Warfare', E EJIL:TALK!, 17 January 2019, https://www.ejiltalk.org/joint-blog-series-sieges-evacuations-and-urban-warfare-thoughts-from-the-transatlantic-workshop-on-international-law-and-armed-conflict/#more-16823
27 See for example Stephen Kalin, 'U.S.-Backed Forces in Syria Move against Last IS Pocket in Baghouz: SDF Official', Reuters, 1 March 2019.
28 See for example ICRC, API, article 82 and 83.
29 See for ROE: example Blaise Cathcart, 'Application of Force and Rules of Engagement in Self-Defence Operations', in T.D. Gill and D. Fleck, eds., The Handbook of the International Law of Military Operations (Oxford: Oxford University Press, 2017), 228: 'The ROE framework ensures that political direction and objectives as well as legal, diplomatic, policy and operational considerations are coherently conveyed in military orders or directives'. For a description of the targeting process, see Philip R. Pratzner, 'The Current Targeting Process', in Ducheine P.A.L., Schmitt, M.N., and Osinga, F.P.B., eds., Targeting: The Challenges of Modern Warfare (The Hague: Asser, 2016), 77–97.
30 Pesha Magid and Shawn Carrié, Destroyed and Saved, the Intercept, 22 April 2018.
31 See, for example, Jamie Merrill, 'EXCLUSIVE: Britain Drops 3,400 Bombs in Syria and Iraq – and Says No Civilians Killed' Middle East Eye, 17 October 2017:

> A source in the RAF told Middle East Eye: 'Given the ruthless and inhuman behavior of our adversary, including the deliberate use of human shields, we must accept that the risk of inadvertent civilian casualties is ever present, particularly in the complex and congested urban environment within which we operate.'

https://www.middleeasteye.net/news/exclusive-britain-drops-3400-bombs-syria-and-iraq-and-says-no-civilians-killed.
32 See for example Martin Chulov, 'US Admits Mosul Airstrikes Killed over 100 Civilians during Battle with Isis', The Guardian, 25 May 2017, https://www.theguardian.com/world/2017/may/25/us-mosul-airstrikes-deadliest-attack-iraq-2003.
33 Van den Boogaard and Vermeer, 'Precautions', 174–176.
34 Marco Sassòli and Anne Quintin, 'Active and Passive Precautions in Air and Missile Warfare', Israel Yearbook on Human Rights 44 (2014), 82.
35 Sandoz et al, Commentary on the Additional Protocols, 692, see also the declaration by the United Kingdom upon ratification, see https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Notification.xsp?action=openDocument&documentId=0A9E03F0F2EE757CC1256402003FB6D2.

36 See for example Susannah George, 'Mosul Is a Graveyard: Final IS Battle Kills 9,000 Civilians', Associated Press, 21 December 2017, https://www.apnews.com/bbea7094fb954838a2fdc11278d65460S.
37 The assumption here is that the planned IDF attacks were proportionate before the warnings were conveyed to the civilian population. If the planned attacks only would be proportionate after the civilians left as a result of the warnings, one may say that the PA indeed helped IDF turn the expected civilian collateral damage from excessive into proportionate.
38 For a concise explanation of the legal limits of lawfare, see Craig Martin, 'What Are the Limits on Lawfare?', Opinio Juris, 5 December 2019, https://opiniojuris.org/2019/05/05/what-are-the-limits-on-lawfare/
39 Ibid.
40 Raphael S. Cohen, Nathan Chandler, Shira Efron, et al., Peering into the Crystal Ball, Holistically Assessing the Future of Warfare (Santa Monica, CA: RAND, 2020), 15.

References

Abu Toameh, Khaled. 'Hamas Says PA Helped Israel Attack Gaza', *Jerusalem Post*, 27 March 2019, https://www.jpost.com/Israel-News/Hamas-PA-helped-Israel-attack-Gaza-584757.

Blank, Laurie R., 'Sieges, Evacuation and Urban Warfare', E *EJIL:TALK!*, 17 January 2019,
https://www.ejiltalk.org/joint-blog-series-sieges-evacuations-and-urban-warfare-thoughts-from-the-transatlantic-workshop-on-international-law-and-armed-conflict/#more-16823.

Boogaard, Jeroen van den, 'Knock on the Roof, Legitimate Warning or Method of Warfare?' *Yearbook of International Humanitarian Law* 19 (2016).

Boogaard, Jeroen van den, and Vermeer, Arjen, 'Precautions in Attack and Urban and Siege Warfare', *Yearbook of International Humanitarian Law* 20 (2019), 163–198.

Cathcart, Blaise, 'Application of Force and Rules of Engagement in Self-Defence Operations', in *The Handbook of the International Law of Military Operations*, T.D. Gill, D. Fleck, eds. (Oxford: Oxford University Press, 2017).

Chulov, Martin, 'US Admits Mosul Airstrikes Killed over 100 Civilians during Battle with Isis', *The Guardian*, 25 May 2017, https://www.theguardian.com/world/2017/may/25/us-mosul-airstrikes-deadliest-attack-iraq-2003.

Cohen, R.S., Chandler, N., Efron, S., et al., *Peering into the Crystal Ball, Holistically Assessing the Future of Warfare* (Santa Monica, CA: RAND, 2020).

Corn, Geoffrey S., 'War, Law, and the Oft Overlooked Value of Process as a Precautionary Measure', *Pepperdine Law Review* 42:3 (2014), 419–466, available at: https://digitalcommons.pepperdine.edu/plr/vol42/iss3/2.

Dunlap, Charles J., 'Introduction to the Concept of Lawfare', *National Security Law*, J. Norton Moore, G.B. Robert, R.F. Turner, eds., 823–838 (Durham: Carolina Academic Press, 2015).

Emanuelle-Chiara Gillard, 'Sieges, the Law and Protecting Civilians', *Chatham House Briefing*, June 2019, https://www.chathamhouse.org/publication/sieges-law-and-protecting-civilians.

George, Susannah, 'Mosul Is a Graveyard: Final IS Battle Kills 9,000 Civilians', *Associated Press*, 21 December 2017, https://www.apnews.com/bbea7094fb954838a2fdc11278d65460S.

Henckaerts, Jenne Marie, and Louise Doswald-Beck, L., *Customary International Humanitarian Law, Volume I: Rules* (Cambridge: Cambridge University Press, 2005).

ICRC, *Additional Protocol I to the Geneva Conventions* (Geneva: ICRC, 1977).

ICRC, *Fourth Geneva Convention* (Geneva: ICRC, 1949).

ICRC, 'New Research Shows Urban Warfare 8 Times More Deadly for Civilians in Syria and Iraq', *News Release*, 1 October 2018.

ICTY, Prosecutor vs. Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, Appeals Chamber, 2 October 1995, para. 70.

Jensen, Eric T., 'Precautions against the Effects of Attacks in Urban Areas', *International Review of the Red Cross* 98:901 (2016), 147–175.

Kalin, Stephen, 'U.S.-backed Forces in Syria Move against last IS Pocket in Baghouz: SDF Official', *Reuters*, 1 March 2019.

Magid, Pesha, and Carrié, Shawn, 'Destroyed and Saved', *The Intercept*, 22 April 22 2018,

https://theintercept.com/2018/04/22/to-defeat-isis-the-u-s-helped-turn-old-mosul-into-rubble-but-wont-help-rebuild-it/

Martin, Craig, 'What Are the Limits on Lawfare?', *Opinio Juris*, 5 December 2019, https://opiniojuris.org/2019/05/05/what-are-the-limits-on-lawfare/.

Merrill, Jamie, 'EXCLUSIVE: Britain Drops 3,400 Bombs in Syria and Iraq – and Says No Civilians Killed' *Middle East Eye*, 17 October 2017, https://www.middleeasteye.net/news/exclusive-britain-drops-3400-bombs-syria-and-iraq-and-says-no-civilians-killed.

Pratzner, Phillip R., 'The Current Targeting Process', in Ducheine P.A.L., Schmitt, M.N., Osinga, F.P.B., eds., *Targeting: The Challenges of Modern Warfare* (The Hague: Asser, 2016), 77–97.

Sandoz, Yves, Swinarski, Christophe, and Zimmerman, Bruno, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: International Committee of the Red Cross, 1987).

Sari, Aurel, 'Urban Warfare: The Obligations of Defenders', *Joint Blog Series*, 28 January 2019, https://blogs.icrc.org/law-and-policy/2019/01/28/joint-blog-series-urban-warfare-the-obligations-of-defenders/.

Sassòli, Marco, and Quintin, Anne, 'Active and Passive Precautions in Air and Missile Warfare', *Israel Yearbook on Human Rights* 44 (2014), 69–123.

Zeitoun, M., and Talhami, M., 'The Impact of Explosive Weapons on Urban Services: Direct and Reverberating Effects across Space and Time', *International Review of the Red Cross*, 98:901 (2016), 53–70.

16 The conduct of lawfare

The case of the Houthi insurgency in the Yemeni civil war

Sandra de Jongh and Martijn Kitzen

Introduction

Although inter-state conflict is again on the rise, the past two decades have been characterized increasingly by asymmetric conflicts with states fighting insurgencies, and vice versa. This global trend includes a diverse range of conflicts and actors varying from complicated regional insurgencies such as the Islamic State to more traditional insurgencies which occurred in the Philippines. Typically, these actors are military less powerful than the states they are facing; yet they somehow succeed to persevere and sometimes even prevail. It is not surprising, therefore, that there is abundant literature on factors contributing to the success (and failure) of insurgencies. This chapter seeks to contribute to this body of knowledge by exploring a particular strand that over recent years has been repeatedly cited as a possible explanation for the survival of insurgencies in the fight against powerful enemies. The persistence of the Taliban *vis-à-vis* the United States, and Hamas against Israel, for instance, has been explained by referring to a method employed by such insurgencies to turn their asymmetrical power-status into an advantage. That specific method is *lawfare*, a concept which encapsulates various means and methods designed to (ab)use the rules and norms inherent to international law as a method of warfare.[1] As such, the concept of lawfare offers insight in the way non-state actors use a double standard for strategic purposes: they leverage humanitarian norms and principles enshrined in international law for their own protection, while they exploit the obligations that bind more powerful actors to their own advantage.

In the previous chapter Van den Boogaard argued from a judicial perspective that 'there is no place for lawfare in armed conflict'. Yet, reality is that lawfare has become endemic to the conduct of modern war. Even state adversaries like China in the South China Sea, Russia in Ukraine, and Iran throughout the Middle East have deployed activities that capitalize Western concern for International Humanitarian Law (IHL).[2] As illustrated by Johnson in Chapter 3, both state and non-state actors might use hybrid tactics without adhering to international conventions. Moreover, by deliberately operating in an ambiguous way, they avoid crossing

the threshold of what is legally considered an act of war (see also Bart Van den Bosch in Chapter 13). Consequently, Western democracies or alliances 'with a high regard for international rules and the rule of law' are facing adversaries that almost continuously seek to exploit this position.[3] Indeed, the spread of lawfare is considered a restraint that deters liberal-democratic states to engage in conflicts.[4] It should be noted that this factor, among others, has contributed to the rising popularity of 'remote' or 'surrogate warfare' in which Western countries outsource much of the burdens of warfare to other (local) parties.[5] All this especially pertains to irregular wars, such as the fight against violent extremism and conflicts that take place in the 'grey zone' between war and peace. In both these types of conflict non-state actors fulfill an important role, either as protagonists or as proxy agents of state adversaries. Hence this analysis focuses on the way non-state opponents seek to employ lawfare in order to gain an advantage in modern warfare.

This chapter applies the concept of lawfare to the Yemeni civil war. The conflict has left the country increasingly fragmented and, despite several offers of de-escalation and peace negotiations, a real political solution to silence the guns is not in sight.[6] Even worse, due to the protracted and particularly vicious character of the conflict humanitarian suffering in Yemen has reached unprecedented levels. Civilians continue to bear the brunt of the failure of the warring parties to negotiate a settlement. Reports detailing the various (war) crimes committed by all sides to the conflict are in abundant supply.[7] Many such reports cite continued attacks on civilian settlements and infrastructure in general, and protected sites specifically.

Despite the dire situation in Yemen, the main insurgent group, the 'Ansar Allah militia' or 'Houthi insurgency' seems far from defeated. On the contrary, the group has become increasingly bold in demonstrating its potency, including by launching attacks into the territory of its main adversary, Saudi Arabia. The survival of the group is remarkable in light of the amount of military firepower directed against it. A Saudi-led coalition consisting of Arab countries capable of deploying a significant and well-equipped military force has been fighting the insurgents in support of the internationally recognized Yemeni government under President (in exile) Hadi.[8] In addition, this alliance is propped up by the United States, the United Kingdom, and France who have continued to supply advanced weaponry for use in the Yemeni campaign.[9] Though the Houthi insurgency itself is also a considerable force – with an estimated strength of circa 180,000–200,000 men, 2.7–3 billion US dollars, and in possession of a considerable arsenal containing missiles and tanks – its capabilities represent but a fraction of those at the disposal of the coalition.[10] This is easily illustrated by the fact that Saudi Arabia alone pledged to contribute some 150,000 soldiers and 100 planes at the start of the counterinsurgency campaign.[11]

The Houthis' survival, despite the insurgency's asymmetrical disadvantage, begs the question as to the reasons behind this relative success.

This chapter explores whether the group's success can – at least in part – be explained by the concept of lawfare. Specifically, it seeks to answer the question as to whether the Houthis have deliberately employed a strategy of lawfare in their insurgent campaign and, if so, to what extent this strategy has contributed to its strategic success. To this purpose, this chapter first explores the theoretical foundations of the lawfare concept. It subsequently provides an analysis of the origins and the goals of the Houthi insurgency followed by an assessment of how the Houthi's use of lawfare has contributed to the group's cause thus far. The conclusion reflects on the wider relevance of this case study's findings and offers insights for the conduct of war in today's world.

Lawfare

In essence lawfare is a concept that can be used to connote both negative and positive uses of the law for achieving military objectives. Some definitions of the concept – indeed – are neutral, and incorporate this dual possibility. Williams, for instance, defines lawfare as the use of law 'with the intent of securing a political or military advantage over the opposing party'.[12] In the majority of cases, however, lawfare is used to depict a more negative undertaking, incorporating into the definition the assumption that lawfare is used for wrongful ends. Goldstein takes such a negative interpretation of lawfare, and has defined it as 'the wrongful manipulation [or] exploitation of the law to achieve a purpose other than or contrary to that for which the law was originally enacted'.[13] Since 'neutral' definitions of lawfare do not distinguish between misuse of the law and the normal functioning of the law as intended (namely to place boundaries on military conduct), we opted to use the latter, negative interpretation as the best workable lens for studying the actual application of lawfare in the conduct of war.

The law can be exploited by an adversary to hurt an opponent in various different ways. In its simplest form, lawfare includes casting unfounded accusations as to the illegality of the actions of the other side, damaging the adversary's legitimacy and exposing him to retaliatory (legal) repercussions.[14] Concretely, a party may orchestrate collateral damage or civilian casualties, and succeed in framing the incident to such an extent that the adversary is (falsely) held responsible.[15] In a more advanced sense, actors may stage deliberate attempts to *induce* their adversary to violate the laws of war *vis-à-vis* themselves and their supporters, including civilians.[16] An example of such behavior is the deliberate positioning of militants and their assets among civilian installations and facilities (such as hospitals and schools) which, if attacked, would induce significant civilian casualties. Actors who have been implicated in doing so include the Taliban, who are known to position military assets in the near vicinity of noncombatant facilities such as hospitals or schools protected by IHL. Key motives for this behavior include the deterrence of attacks, and, in the case that attack does follow

through, substantial collateral damage that reflects badly upon the United States or other involved coalition partners.[17] Another example of a successful strategy involving lawfare is the embedding of Palestinian militants or military assets within civilian installations such as mosques, schools, or hospitals.[18] When the Israeli Defense Forces proceed to attack such facilities, it is them who face the consequences of international condemnation and legal inquiries, whereas those actors who deliberately orchestrate such situations are left relatively untouched.[19] Lawfare, thereby, might be considered a form of effects-based warfare focusing on the effect created by this particular *modus operandi*, whereas the means used to obtain such effects are of subordinate importance.

The aforementioned examples all illustrate that lawfare offers a powerful tool to parties – such as insurgencies – who are unable to overpower their adversary militarily, and therefore seek to engage their adversary's specific vulnerabilities.[20] In the case of (intervening) Western democracies, those vulnerabilities predominantly relate to the damaging potential that public opinion may have on political resolve and the continuity of military operations.[21] As Eckhardt explains:

> Knowing that our society so respects the rule of law that it demands compliance with it, our enemies carefully attack our military plans as illegal and immoral and our execution of those plans as contrary to the law of war.[22]

These 'enemies' are less vulnerable to condemnation and critique when they do so, again by virtue of the asymmetric unbalance which precludes them from being held accountable to the norms and rules of international law that function to condition the behavior of states.[23]

A successful lawfare campaign can have various (tactical and/or strategic) outcomes (see Table 16.1).[24] First of all, a successful lawfare strategy can attain tactical successes *inter alia* by delegitimizing some (or all) of the opponent's means and methods of warfare as and thereby deeming them off-limits. Another lawfare-enabled tactical advantage includes deterring adversaries from attacking hideouts or important caches due to the risk of

Table 16.1 Lawfare Methods and Outcomes

Approach	*Key Activity*	*Tactical Outcomes*	*Strategic Outcomes*
Delegitimization	Orchestrating and framing of (false) accusations	Restraining an opponent's means and methods	Undermining of support and political will
Deterrence	Positioning of assets in the vicinity of civilians and noncombat facilities	Protection of assets Inducement of violations	Undermining of support and political will

collateral damage.[25] At a strategic level the utility of lawfare lies in accomplishing the goal of undermining public support for military campaigns, an indispensable component of the will to conduct and endure military operations – especially in democratic societies where the decision to go to and continue a war is made under severe public scrutiny. Lawfare succeeds in doing so when it makes it appear that a country is engaged in an aggressive and illegitimate military campaign that is in violation of international law.[26] More tangibly, the use of lawfare in this way will result in widely publicized collateral damage and civilian casualties. In many cases, the accusations are repeated without thorough legal analysis. Even though such casualties would be the insurgent's intended result, they reflect detrimentally upon the state-adversary, since he is the one who is held accountable under international law. Indeed, if lawfare is successful, an insurgent manages to portray itself as victim, and the actor as aggressor, which delegitimizes the state's campaign.[27]

Ansar Allah: the Houthi insurgency

The civil war in Yemen must be understood as the result of an enduring competition within Yemeni society over which actor gets to control the state.[28] This power struggle is characterized by deep-rooted political inequalities and divisive patronage relationships with the country's most potent social forces, the tribes, as key players.[29] Regime stability in Yemen has historically suffered from threats to its monopoly on the legitimate use of force, posed by various tribes.[30] Under the rule of former President Saleh the tribes in predominantly the northern part of Yemen, representing the middle and lower classes, faced continuous political and socio-economic marginalization. Whereas the southern region prospered, the north remained relatively underdeveloped and people were suffering hardship. Under the leadership of the Houthi family various northern tribes began to resist the state's discriminatory policy which in 2004 resulted in the first Houthi war.[31] This definitely established the Houthi-led northern tribal alliance as an armed insurgency that, from then onwards succeeded in undermining the authority and legitimacy of the national government.[32]

The Yemeni state effectively crumbled in 2011 when president Saleh was ousted by Vice-President Hadi. The Houthi alliance grasped the opportunity to expel government forces and wrest control over their tribal heartlands in the north. Subsequent efforts to negotiate with and agree upon a transitional agreement of national unity failed. A main source of this failure was the inability to properly address key players' concerns within the proposed settlement. More specifically, the Houthis felt underrepresented at the negotiations, and feared outcomes – such as federalization – that would diminish the power of their tribe within the northern territories.[33] These concerns were reinforced by UN Security Council resolution 2216 (2015), which called for the effective surrender of the Houthis, imploring them to

hand back control to the Hadi government.[34] Subsequently, Houthi militias took up their weapons again and staged a *de facto* coup in which they seized the city of Sanaa, dissolved parliament, and forced Hadi to resign.[35] Due to their close cooperation with former president Saleh, the insurgency profited from 'the absorption of entire brigade sets of tanks, artillery, and anti-aircraft weapons' as well as strategic missiles, coastal defenses, and additional intelligence capabilities in its military apparatus.[36] Hadi managed to escape to Saudi Arabia, where he not only found shelter but also encountered the Kingdom's willingness to intervene in the Yemen civil war on behalf of his government.[37] This ushered the start of the Saudi-led invasion after which the conflict ensued in full intensity.

The insurgency's background demonstrates how the dominant 'sectarian proxy-war' frame used to depict Yemen's conflict by the media is at least a severe simplification and more probably seriously flawed; the Houthis first and foremost are an insurgency vying to secure its interest in the ongoing Yemeni power struggle.[38] Indeed, since Houthi grievances originally were of a local and political character, the core of the movement's political-military strategy rests upon the pursuit of self-determination. Ultimately, their strategic goal is to conclude a favorable political settlement that awards them their desired degree of power and resources.[39] Sectarian motives, therefore, have never been at the heart of the insurgency.[40] Yet, the Yemeni civil war is almost continuously delineated as a conflict following Islam's Sunni-Shi'a cleavage, with the Shi'ite Houthis as an Iranian proxy pitched against the predominantly Sunni coalition led by Saudi Arabia. We take the stance, however, that despite abundant support from Iran, the Houthis should not be primarily regarded as an Iranian proxy as they cherish their own independent goals and aspirations regarding political power and control over local resources.[41] A UN panel of experts monitoring the arms embargo imposed on Yemen seems to support this view as it has reported limited Iranian involvement, stating that albeit there is little doubt that Iran has provided supplies to the insurgency, the existence of direct financial or military support could not be confirmed.[42] Moreover, the Houthis have repeatedly emphasized their pursuit of ending Yemen's corrupt and ineffective national government and their desire to provide an alternative political solution.[43] The current Houthi military influence and territorial disposition thus serve as a leverage to broker these desired outcomes and thus secure substantial *political* gains. Let us now see to what extent the Houthis have employed lawfare during their campaign and how this has contributed to obtaining the movement's strategic goals.

The Houthis' conduct of lawfare: practice and effect

International law, in particular IHL, serves to condition the use of force in order to minimize civilian harm and humanitarian suffering. The Geneva Conventions, for instance, bestow special protections upon designated

areas, such as hospitals, schools and places of worship, and obligate parties to, *inter alia*, do their utmost to minimize the potential for collateral damage when conducting attacks. Violations of the rules and principles of IHL are considered especially egregious, and may often amount to war crimes. In a conflict setting, parties should therefore conduct themselves in an IHL-compliant manner, or risk facing serious consequences. Yet, throughout their military campaign, the Houthis have not shunned away from getting their hands dirty and violating those rules and principles of IHL.

In addition to deliberate attacks on civilian infrastructure and settlements, the Houthis have exploited humanitarian law by using 'human-shields': the positioning of military assets and militants within or in the vicinity of protected civilian sites.[44] Indeed, more incidents incite suspicions of a recurring pattern whereby the Houthis have purposefully erected military facilities in the vicinity of (protected) civilian sites such as schools, hospitals and detention centers in an effort to deter coalition attacks.[45] In case such objects qualify as military objectives, they might lose their protection against attack. In one incident in 2015, for instance, the insurgents had co-located a detention center with a military storage facility for weapons such as anti-aircraft guns. The site was subsequently considered a military objective and targeted by a coalition airstrike on 21 May 2015, killing the 11 detainees who were reportedly there as human shield.[46] In another incident Houthi insurgents forced their entry into a medical facility, ordered the majority of the staff to vacate the premises, and pursued to utilize the facility for military purposes from 1 to 7 November 2018.

More recently, various reports have also cited that the insurgents deliberately transferred an estimated number of 400 captives from a detention center to a military facility in Sanaa. This specific facility had been frequently subjected to coalition bombings, and the main purpose of the move of prisoners, therefore, was to deter any new strikes in the future.[47] In a particularly infamous incident in September 2019, coalition planes struck a Houthi-managed detention center, killing at least 100 detainees. This invoked strong criticism against the Saudi-led coalition for what was deemed an illegitimate indiscriminate attack on a protected site. However, although the Houthis have always denied using the site as a military facility, various prisoners have since then attested to the fact that the site was used to store weapons.[48]

These examples indicate that the widespread and recurring use of the practice of 'hugging' or exploiting civilian sites for military purposes by the Houthis points at a deliberate pattern. This conclusion has been repeatedly echoed in the annual reports of the UN Panel of Experts on Yemen, which identified sufficient testimony to speak of a purposely crafted strategy of abuse of IHL.[49] All in all, these practices leave little doubt that the Houthis have employed lawfare during their campaign. Indeed, in particular IHL has been exploited in a way contrary to its intentions, but to what effect?

Lawfare seems not only to be systematically embedded in the Houthi insurgency's conduct of war, but it also appears to serve both tactical and

strategic purposes. To start with the former, the use of lawfare by the Houthis has bestowed upon the movement's fighters a certain level of protection by concealing them within humanitarian facilities, thereby establishing a level of deterrence against airstrikes by the Saudi-led coalition, limiting the coalition's warfare toolbox.[50] However, the coalition has repeatedly shown the resolve not to recoil from bombing such protected targets categorically. Even when extensive collateral damage followed – and accusations of disproportional and indistinct attacks ensued – the coalition has continued to strike Houthi military facilities hidden among the population. Nevertheless, while results vary, this widely used Houthi-tactic forced the coalition to carefully consider its targeting process. Arguably, each case in which the Houthis have succeeded in co-opting humanitarian sites without being subjected to attack is testament to the tactical success of their lawfare strategy.

The *strategic* effect of Houthi lawfare is intertwined with its tactical utility. Emphasizing the innocent victims fallen as a result of coalition operations has turned out to function as a particularly powerful tool of political messaging capable of delegitimizing the (actions of) the Saudi-led alliance as well as its Western supporters.[51] Obviously, this narrative has gained traction and is, among others, repeatedly echoed in the collective body of UN reports on Yemen. Even the overall trend in Western media outlets reveals a tendency to focus on the numerous incidents – and their second-order humanitarian effects– whereby civilian installations such as humanitarian shelters, medical facilities, and schools have been targeted by the Saudi-led campaign. The coalition itself has always responded by following the line of argumentation that due to the presence of Houthi fighters or weapons systems all of its actions against civilian sites have been legitimate as they aim to target military objectives in order to diminish the insurgent's fighting capabilities. Despite this consistent messaging, the coalition has been unsuccessful in reshaping the narrative toward the detriment of the Houthis. On the contrary, as mentioned earlier the Saudi-led alliance bears the brunt of the media, UN and NGO's accusations in relation to IHL and International Human Rights Law (IHRL) violations. Much less mention, in his regard, is made of Houthi responsibility. As such, this strategic effect of Houthi lawfare taps into a critical vulnerability which also extends to the coalition's political supporters who have provided financial resources and supplied (sophisticated) arms. Consequently, UN reports as well as civil society groups have repeatedly called upon the United States, the United Kingdom, and France – among others – to halt their support for the coalition's war effort.

So, how to assess the success of the Houthi lawfare campaign? Ultimately the insurgents fight to secure their strategic goals of political inclusion and resource sharing; the question, therefore, is how the conduct of lawfare has contributed to these goals. As described in the theoretical framework lawfare is successful if the party using it succeeds in presenting its adversary as the aggressor, and itself as the victim. Albeit that the Houthis have succeeded in achieving the former, they have been less successful regarding the latter. The

movement itself has also received severe criticism for deliberately attacking civilian infrastructure and for putting civilians in harm's way, violations for which there is abundant (UN-backed) evidence.[52] It seems that targeting civilians – including in airports, villages, and refugee camps – has become a goal by itself rather than an unwanted side effect of the deployed strategy.[53] In addition, the insurgents have also gradually increased their attacks on civilian infrastructure in Saudi Arabia.[54] In its latest report, the UN Panel of Experts on Yemen, therefore, has explicitly denounced the Houthis as they 'demonstrated a frequent disrespect for international humanitarian law as applied to the protection of humanitarian relief staff, health-care personnel and health-care infrastructure'.[55] This claim is supported by evidence of numerous incidents including the indiscriminate use of explosive weapons such as mortars and artillery shells in densely populated areas, for which the UN Panel was unable to identify military objectives justifying the degree of collateral damage and civilian death toll.[56] These accusations are harmful to the insurgency in the long-term, and might jeopardize the prospects at power-sharing as the international community (whose rules and norms have been violated) most probably will play an important role in brokering a peace settlement. As of yet, however, peace negotiations are still ongoing and due to their prominent position in the conflict the Houthis have a clear seat at the table. Nevertheless, Houthi leadership has recently started to demonstrate significant signals of its willingness to de-escalate and reach a political settlement. Reportedly various political prisoners have been released and the frequency of strikes into Saudi(-controlled) territory has been reduced.[57] This may indicate that the Houthis feel that their strategic goals are within arms' reach as they now have gained sufficient leverage to secure commitments leading to a power-sharing arrangement with inclusion of Houthi-affiliated tribes. In order to capitalize on this desired outcome, it is essential to build a reputation of trustworthiness. Consequently, preventing a backfire on their strategic long-term goals requires the Houthis to abandon lawfare practices rather sooner than later.

In the end, this case study has brought to light that the Houthis indeed have repeatedly employed lawfare tactics as part of their campaign in the Yemeni civil war. While the militants clearly have not shied away from violating the rules and principles of international right in general, a particular strong and recurring pattern can be discerned with regard to the exploitation of civilian and protected sites for military purposes. According to our assessment this conduct of lawfare has brought the Houthi movement not only considerable tactical advantages but also strategic-level outcomes, where it triggered rigorous scrutiny of the conduct of the Saudi-led coalition and its (non-)adherence to international law. In this regard, Houthi lawfare has been particularly successful. This success, however, also came at a prize for the insurgents. Whereas theoretically lawfare should also serve to picture weaker parties as victims *vis-à-vis* more powerful opponents, the Houthis have failed to achieve this. They have accomplished the contrary

as they are currently regarded as a party that – at least – has been complicit in one of the world's worst humanitarian disasters to date. Consequently, the Houthis themselves have been subject of international condemnation for their systematic violations of international humanitarian law. We consider this an – in the eyes of the Houthis – undesired and detrimental strategic effect of tactical lawfare, which potentially holds serious backfiring implications endangering the attainment of the insurgents' overall strategic goals. Hence, we assess that if Houthi leadership considers the group's current position sufficiently strong for cutting a deal that could realize their long-wished aims (of power-sharing at the national level and authority over their territories in northern Yemen), it will most probably step down its use of tactical lawfare in order to prove itself a trustworthy partner. Whereas the conduct of lawfare has certainly contributed to Houthi survival and tactical battle field success thus far, more collaborative and moderate behavior is instrumental for consolidating this in strategic success in the form of a durable peace agreement.

Conclusion

As a singular case study this analysis of Houthi warfare holds limited value for drawing more general conclusions. Yet, there are insights can serve to advance the understanding of the utility of lawfare in the conduct of modern war as they offer an avenue for further research. First, the case calls for a better understanding of the relationship between (the lack of) strategic and tactical effects of lawfare. The group's failure to convey the image of themselves as victims points in a structural direction; does application of lawfare inherently require maintaining the equilibrium between violations of international rules for tactical advantages and effective strategic communication to exploit such acts for strategic gains? A comparative study that digs into this issue might be particularly helpful for designing measures that can mitigate or even thwart an opponent's use of lawfare. Second, the Houthi case has highlighted that actors who deploy lawfare at a more advanced stage of their campaign might need to transform from vicious violators of international rules and principles into trustworthy partners for settling negotiations. This holds potentially wider complications as it offers a concrete strand for countering lawfare by opponents who pursue goals that can be accommodated in peace agreements. If this is the case, our findings seem to suggest that ultimately reputation management matters more than the use of messy tactical tricks. An enhanced understanding of this dynamic might lead to the adoption of methods that force opponents to adjust their 'strategic timing' and abandon the conduct of lawfare at an earlier stage of the conflict as they come to realize that this might jeopardize the attainment of their strategic goals.

Where does this leave us with regard to the impact on the conduct of war? As mentioned in the introduction the spread of lawfare acts as a restraint

that is partially responsible for the limited nature of current Western interventions in violent conflicts. From the perspective of liberal democracies, after all, it is pivotal to prevent being portrayed as violators of international law. While this trend is expected to continue into the near future, the insights of this chapter demonstrate that the conduct of lawfare itself is not infallible or without risk to actors deploying the concept. Especially when they fail in effectively victimizing themselves or take their lawfare practices too far – either in extent or time – this might trigger a backlash that obstructs the attainment of strategic goals. Western states, therefore, should not only develop methods for dealing with lawfare, but first and foremost they should play into their strength by exploiting their adherence to international law and norms in the conduct of war. Or to paraphrase Van den Boogaard's statement from the previous chapter, there is no place for lawfare in armed conflict as far as this concerns contributions that are the result of Western interventions. At the tactical level this might be perceived as a disadvantage as it leads to restrictions with regard to the use of force; yet it bolsters the ability to withstand strategic effects of lawfare as it allows for credibly conveying the message that one strictly acts in accordance with international law. This, however, is easier said than done as it requires much more than investing in effective strategic communication. In the context of modern warfare, it also involves resisting the temptation to counter illegal activities below the threshold of war with similar hybrid tactics. Moreover, it also boils down to successfully impressing this view in (local) allies who might have very different standards. Especially this latter point seems to become more and more urgent as remote and surrogate warfare have become increasingly significant for fighting violent extremism as well as for the global competition for influence. Thus, in order to shield Western interventions against lawfare, all allied actors should adhere to the preponderance of international law in their conduct of war. Any strategy in modern warfare, therefore, should consider and address the salient issues of law(fare) in a specific conflict.

Notes

1 Gabriella Blum, 'On a Differential Law of War', Harvard International Law Journal 52 (2011), 164–218.
2 IHL is also known as Law of Armed Conflict. In concurrence with the previous chapters we have opted to use the term IHL.
3 David Kilcullen, 'The Evolution of Unconventional Warfare', Scandinavian Journal of Military Studies 2:1 (2019), 68.
4 Raphael S. Cohen, Nathan Chandler, Shira Efron, et al., Peering into the Crystal Ball, Holistically Assessing the Future of Warfare (Santa Monica, CA: RAND, 2020), 10, 16–17, 19.
5 For 'remote and 'surrogate warfare' see, respectively, Emily Knowles and Abigail Watson, Remote Warfare, Lessons Learned from Contemporary Theatres (London: Oxford Research Group, 2018), Andreas Krieg and Jean-Marc Rickli, Surrogate Warfare, The Transformation of War in the Twenty-First Century (Washington, DC: Georgetown University Press, 2019).

6 See, among others, Peter Salisbury, 'What Does the Stockholm Agreement Mean for Yemen?', The Washington Post, 21 December 2018, available at https://www.washingtonpost.com/news/monkey-cage/wp/2018/12/21/what-does-the-stockholm-agreement-mean-for-yemen/, and April Longley Alley, 'How to End the War in Yemen', Foreign Policy, 15 October 2019, available at https://foreignpolicy.com/2019/10/15/yemen-houthis-saudi-arabia-end-war/.
7 See for instance the 2018 and 2019 reports of the Group of Eminent Experts on Yemen, mandated by the Human Rights Council (https://www.ohchr.org/EN/HRBodies/HRC/YemenGEE/Pages/Index.aspx).
8 The coalition first intervened in 2015 and in addition to Saudi Arabia troop contributions have been provided by Bahrain, Egypt, Jordan, Kuwait, Morocco (until 2019), Qatar (until 2017), Sudan (until 2019), and the United Arab Emirates.
9 Office of the High Commissioner on Human Rights (OHCHR), Yemen: Collective Failure, Collective Responsibility (Geneva: OCHCR, 2019), available at https://www.ohchr.org/EN/HRBodies/HRC/ YemenGEE/Pages/Index.aspx, 218.
10 Renaud Mansour and Peter Salisbury, Between Order and Chaos: A New Approach to Stalled State Transformations in Iraq and Yemen (London: Chatham House, 2019), 22–23.
11 Steve Almasy and Jason Hanna, 'Saudi Arabia Launches Air Strikes in Yemen', CNN, 26 March 2015, available at https://edition.cnn.com/2015/03/25/middleeast/yemen-unrest/.
12 Paul R. Williams, 'Lawfare: A War Worth Fighting', Case Western Reserve Journal of International Law 43:1–2, 145.
13 Brook Goldstein, International and Domestic Legal Resources: Responding to Lawfare and the Goldstone Report (Speech, Fordham Law School, New York, 27 April 2010).
14 David Luban, 'Carl Schmitt and the Critique of Lawfare', Case Western Reserve Journal of International Law 43:1–2 (2010), 457.
15 Michael Sharf and Elizabeth Andersen, 'Is Lawfare Worth Defending? Report of the Cleveland Experts Meeting', Case Western Reserve Journal of International Law 43:1–2 (2010), 13.
16 Charles J. Dunlap, 'Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts' (Conference Paper, Washington DC, 2001), available at https://people.duke.edu/~pfeaver/dunlap.pdf.
17 Orde. F. Kittrie, 'Lawfare and U.S. National Security', Case Western Reserve Journal of International Law 43:1–2 (2010), 369.
18 Anthony H. Cordesman, The 'Gaza War': A Strategic Analysis (Washington, DC: CSIS, 2009), available at https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/090202_gaza_war.pdf, 2.
19 Laurie R. Blank, 'Finding Facts but Missing the Law: The Goldstone Report, Gaza and Lawfare', Case Western Reserve Journal of International Law 43:1–2 (2010), 304.
20 David J.R. Frakt, 'Lawfare and Counterlawfare: The Demonization of the Gitmo Bar and other Legal Strategies in the War on Terror', Case Western Reserve Journal of International Law 43:1–2 (2010), 340.
21 William George Eckhardt, 'Lawyering for Uncle Sam When He Draws His Sword', Chicago Journal of International Law 4:2 (2003), 431–441.
22 Ibid.
23 Avihai Mandlebit, 'Lawfare: The Legal Front of the IDF', Military and Strategic Affairs 4:1 (2012), 52. Of course, the last decade has repeatedly shown that more authoritarian states like Russia or China do not necessarily abide to the internationally agreed pattern of rules and norms. Yet, these states can be confronted with this behavior through diplomatic channels and international institutions. In case of violent non-state actors such mechanism is virtually non-existent.

24 Kittrie, 'Lawfare and U.S. National Security', 396.
25 Luban, 'Carl Schmitt and the Critique of Lawfare', 462.
26 Dunlap, 'Law and Military Interventions', 4.
27 Ami Ayalon, Elad Popovich, and Moran Yarchi, 'From Warfare to Imagefare: How States Should Manage Asymmetric Conflicts with Extensive Media Coverage', Terrorism and Political Violence 28:2 (2016), 264.
28 Maria-Louise Clausen, 'Competing for Control over the State: The Case of Yemen', Small Wars & Insurgencies 29:3 (2018), 571.
29 Brian M. Perkins, 'Yemen: Between Revolution and Regression', Studies in Conflict & Terrorism 40:4 (2017), 314.
30 Ibid., 304.
31 Michael Knights, 'The Houthi War Machine: From Guerilla War to State Capture', CTC Sentinel 11:8 (2018), 15–16, available at https://ctc.usma.edu/app/uploads/2018/09/CTC-SENTINEL-092018.pdf.
32 Asher Orkaby, 'Yemen's Humanitarian Nightmare: The Real Roots of the Conflict', Foreign Affairs 96:6 (2017), 94–95.
33 Thomas Juneau, 'Iran's Policy towards the Houthi's in Yemen: A limited return on a modest investment', International Affairs 92:3 (2016), 653, Perkins, B.M., 'Yemen', 311.
34 United Nations Security Council, Resolution 2216 (S/RES/2216), 14 April 2015.
35 Orkaby, 'Yemen's Humanitarian Nightmare', 96–97.
36 Knights, 'The Houthi War Machine', 17.
37 Mansour, and Salisbury, Between Order and Chaos, 13.
38 Perkins, 'Yemen', 301.
39 Juneau, 'Iran's Policy towards the Houthi's in Yemen', 652.
40 Elisabeth Kendall, Iran's Fingerprints in Yemen. Real Or Imagined? (Washington, DC: Atlantic Council, 2017), 2.
41 Juneau, 'Iran's Policy towards the Houthi's in Yemen', 647.
42 United Nations Security Council (UNSC), Final Report of the Panel of Experts on Yemen (2015) (New York: UNSC, 2016), available at https://www.undocs.org/S/2018/192.
43 Juneau, 'Iran's Policy towards the Houthi's in Yemen', 652.
44 Michelle Nichols, 'Exclusive: U.N. Report on Yemen Says Houthis Used Human Shields, Islamic State Got Cash', Reuters, 4 August 2016, available at https://www.reuters.com/article/us-yemen-security-un-exclusive/exclusive-u-n-report-on-yemen-says-houthis-used-human-shields-islamic-state-got-cash-idUSKCN-10F28B, (UNSC), Final report of the Panel of Experts on Yemen (2015).
45 N. Cumming-Bruce, 'War Crimes Committed by Both Sides in Yemen, U.N. Panel Says', New York Times, 3 September 2019, available at https://www.nytimes.com/2019/09/03/world/middleeast/war-crimes-yemen.html. See also Associated Press, 'Saudi-led Air Strikes in Yemen Kill More than 100 Prisoners', France 24, 2 September 2019, available at https://www.france24.com/en/20190902-yemen-saudi-airstrikes-houthi-prisoners, Dennis M.L.G. Lemmens and Fleur J.M. de Boer, 'The Protection of Schools Under International Humanitarian Law', Militair Rechterlijk Tijdschrift 112:2 (2019), available at https://puc.overheid.nl/mrt/doc/PUC_287624_11/1/.
46 Yemeni Coalition to Monitor Human Rights Violations, (YCMHRV), YCMHRV Report (September 2015), available at: https://reliefweb.int/report/yemen/international-report-documents-crimes-committed-al-houthi-militia-saleh-group-report.
47 Anonymous, 'Human Right Group Accuses Houthis of Using 400 Abductees as Human Shields', Asharq Al-Awsat, 15 October 2019, https://aawsat.com/english/home/article/1946451/human-rights-group-accuses-houthis-using-400-abductees-human-shields.

48 Associated Press, 'Saudi-led Air Strikes in Yemen Kill More than 100 Prisoners'.
49 (UNSC), Final Report of the Panel of Experts on Yemen (2015, 2016, 2017, 2018).
50 United Nations Security Council (UNSC), Final Report of the Panel of Experts on Yemen (2018) (UNSC: New York, 2019), https://undocs.org/en/S/2019/83, Annex 37.
51 Mansour and Salisbury, Between Order and Chaos, 41.
52 OHCHR, Yemen, 13.
53 For an extended, monthly updated oversight see The Yemen Peace Project, War Crimes Tracker, available at https://www.yemenpeaceproject.org/warcrimes.
54 See Counter Extremism Project, Houthis, available at https://www.counterextremism.com/threat/houthis.
55 UNSC, Final Report of the Panel of Experts on Yemen (2018), 4.
56 Ibid., Annex 35.
57 April Longley Alley, 'How to End the War in Yemen', Foreign Policy, 15 October 2019, available at https://foreignpolicy.com/2019/10/15/yemen-houthis-saudi-arabia-end-war/.

References

Almasy, S., and Hanna, J., 'Saudi Arabia Launches Air Strikes in Yemen', *CNN*, 26 March 2015, available at https://edition.cnn.com/2015/03/25/middleeast/yemen-unrest/.

Anonymous, 'Human Right Group Accuses Houthis of Using 400 Abductees as Human Shields', s*Asharq Al-Awsat*, 15 October 2019, https://aawsat.com/english/home/article/1946451/human-rights-group-accuses-houthis-using-400-abductees-human-shields.

Associated Press, 'Saudi-led Air Strikes in Yemen Kill More than 100 Prisoners', *France 24*, 2 September 2019, available at https://www.france24.com/en/20190902-yemen-saudi-airstrikes-houthi-prisoners.

Ayalon, A., Popovich, E., and Yarchi, M., 'From Warfare to Imagefare: How States Should Manage Asymmetric Conflicts with Extensive Media Coverage', *Terrorism and Political Violence* 28:2 (2016), 254–273.

Blank, L.R., 'Finding Facts but Missing the Law: The Goldstone Report, Gaza and Lawfare', *Case Western Reserve Journal of International Law* 43:1–2 (2010), 279–305.

Blum, G., 'On a Differential Law of War', *Harvard International Law Journal* 52 (2011), 164–218.

Clausen, M.L., 'Competing for Control over the State: The Case of Yemen', *Small Wars & Insurgencies* 29:3 (2018), 560–578.

Cohen, R.S., Chandler, N., Efron, S., et al., *Peering into the Crystal Ball, Holistically Assessing the Future of Warfare* (Santa Monica, CA: RAND, 2020).

Cordesman, A. H. (2009), *The 'Gaza War': A Strategic Analysis* (Washington, DC: CSIS, 2009), available at https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/ 090202_gaza_war.pdf.

Counter Extremism Project, *Houthis*, available at https://www.counterextremism.com/threat/houthis.

Cumming-Bruce, N., 'War Crimes Committed by Both Sides in Yemen, U.N. Panel Says', *New York Times*, 3 September 2019, available at https://www.nytimes.com/2019/09/03/world/middleeast/war-crimes-yemen.html.

Dunlap, C. J., 'Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts' (Conference Paper, Washington DC, 2001), available at https://people.duke.edu/~pfeaver/dunlap.pdf.

Eckhardt, William George, 'Lawyering for Uncle Sam When He Draws His Sword', *Chicago Journal of International Law* 4:2 (2003), 431–444, available at https://chicagounbound.uchicago.edu/cjil/vol4/iss2/12/

Frakt, D.L.R, 'Lawfare and Counterlawfare: The Demonization of the Gitmo Bar and other Legal Strategies in the War on Terror', *Case Western Reserve Journal of International Law* 43:1–2 (2010), 335–356.

Goldstein, B., *International and Domestic Legal Resources: Responding to Lawfare and the Goldstone Report* (Speech, Fordham Law School, New York, 27 April 2010).

Juneau, T., 'Iran's Policy towards the Houthi's in Yemen: A Limited Return on a Modest Investment', *International Affairs* 92:3 (2016), 647–663.

Kendall, E., *Iran's Fingerprints in Yemen. Real or Imagined?* (Washington, DC: Atlantic Council, 2017).

Kilcullen, D., 'The Evolution of Unconventional Warfare', *Scandinavian Journal of Military Studies* 2:1 (2019)

Kittrie, O.F., 'Lawfare and U.S. National Security', *Case Western Reserve Journal of International Law* 43:1–2 (2010), 393–421.

Knights, M., 'The Houthi War Machine: From Guerilla War to State Capture', *CTC Sentinel* 11:8 (2018), 15–23, available at https://ctc.usma.edu/app/uploads/2018/09/CTC-SENTINEL-092018.pdf.

Knowles, E., and Watson, A., *Remote Warfare, Lessons Learned from Contemporary Theatres* (London: Oxford Research Group, 2018).

Krieg, A., and Rickli, J.M., *Surrogate Warfare, the Transformation of War in the Twenty-First Century* (Washington, DC: Georgetown University Press, 2019).

Lemmens, D.M.L.G., and De Boer, F.J.M., 'The Protection of Schools under International Humanitarian Law', *Militair Rechterlijk Tijdschrift* 112:2 (2019), available at https://puc.overheid.nl/mrt/doc/PUC_287624_11/1/.

Lis, A., 'Yemen is a Battleground in Iran's Proxy War against the U.S. and Saudi Arabia', *Global Security Review,* 2 October 2019, available at https://globalsecurityreview.com/yemen-iran-proxy-war/.

Longley Alley, A., 'How to End the War in Yemen', *Foreign Policy*, 15 October 2019, available at https://foreignpolicy.com/2019/10/15/yemen-houthis-saudi-arabia-end-war/

Luban, D., 'Carl Schmitt and the Critique of Lawfare', *Case Western Reserve Journal of International Law* 43:1–2 (2010), 457–472.

Mandlebit, A., 'Lawfare: The Legal Front of the IDF', *Military and Strategic Affairs* 4:1 (2012), 51–57.

Mansour, R., and Salisbury, P., *Between Order and Chaos: A New Approach to Stalled State Transformations in Iraq and Yemen* (London: Chatham House, 2019).

Nichols, M., 'Exclusive: U.N. Report on Yemen Says Houthis Used Human Shields, Islamic State Got Cash', *Reuters*, 4 August 2016, available at https://www.reuters.com/article/us-yemen-security-un-exclusive/exclusive-u-n-report-on-yemen-says-houthis-used-human-shields-islamic-state-got-cash-idUSKCN10F28B.

Office of the High Commissioner on Human Rights (OHCHR), *Yemen: Collective Failure, Collective Responsibility* (Geneva: OCHCR, 2019), available at https://www.ohchr.org/EN/HRBodies/HRC/ YemenGEE/Pages/Index.aspx.

Orkaby, A., 'Yemen's Humanitarian Nightmare: The Real Roots of the Conflict', *Foreign Affairs* 96:6 (2017), 93–101.

Perkins, B.M., 'Yemen: Between Revolution and Regression', *Studies in Conflict & Terrorism* 40:4 (2017), 300–317.

Salisbury, P., 'What Does the Stockholm Agreement Mean for Yemen?', *The Washington Post*, 21 December 2018, available at https://www.washingtonpost.com/news/monkey-cage/wp/2018/12/21/ what-does-the-stockholm-agreement-mean-for-yemen/.

Sharf, M., and Andersen, E., 'Is Lawfare Worth Defending? Report of the Cleveland Experts Meeting', *Case Western Reserve Journal of International Law* 43:1–2 (2010), 11–27.

The Yemen Peace Project, *War Crimes Tracker*, available at https://www.yemenpeaceproject.org/warcrimes.

United Nations Security Council (UNSC), *Final Report of the Panel of Experts on Yemen (2015)* (New York: UNSC, 2016), available at https://www.undocs.org/S/2018/192.

United Nations Security Council (UNSC), *Final Report of the Panel of Experts on Yemen (2016)* (New York: UNSC, 2017), available at https://undocs.org/en/S/2019/83.

United Nations Security Council (UNSC), *Final Report of the Panel of Experts on Yemen (2017)* (New York: UNSC, 2018), available at http://www.undocs.org/en/S/2018/594.

United Nations Security Council (UNSC), *Final Report of the Panel of Experts on Yemen (2018)* (New York: UNSC, 2019), available at https://undocs.org/en/S/2019/83.

United Nations Security Council, *Resolution 2216* (S/RES/2216), 14 April 2015, available at https://www.undocs.org/S/RES/2216%20(2015).

Williams, P.R., 'Lawfare: A War Worth Fighting', *Case Western Reserve Journal of International Law* 43:1–2 (2010), 145–152.

Yemeni Coalition to Monitor Human Rights Violations, (YCMHRV), *YCMHRV Report* (September 2015), available at https://reliefweb.int/report/yemen/international-report-documents-crimes-committed-al-houthi-militia-saleh-group-report.

Part VII

Decision-making and war

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

17 Command in the operational dimension

Challenges of the information age

Rob Johnson

Introduction

Critics have suggested that there is a 'crisis' in the operational dimension.[1] Confronted by insurgency, unconventional warfare, overwhelming volumes of data, or the constraints imposed by cautious political leaders under intense media and legal scrutiny, operational commanders face great complexity. Some advocate information operations (IOs) should now take precedence over kinetic actions but the 2010s proved that high-intensity conventional warfare can still occur. The US military solution is for operational commanders to integrate information activities, fully automated weapon systems, robotic logistics tools, and schemes for delivery of fires in Multi-Domain Operations (MDO).[2]

Operational commanders need to consider a great variety of conditions in armed conflict, from land stabilisation tasks to high speed air or naval combat. Operations also demand ethical and professional judgements about the use of emerging technologies. They need to contemplate how operational principles or practice could change if, for example, commanders would have to place human personnel in the path of danger when their order of battle consists largely of robotic vessels, airframes, and ground mobile weapon and communications platforms. Some things are, of course, perennial and will remain, namely, time constraints, prioritisation, the frictions of organisation, rules of engagement, multiple lines of operation, span of command, and reporting chains. Coalition management, where rules of engagement and national policies are different, still cause problems in co-ordination. Nevertheless, one of the most significant demands on commanders in recent years is integrating networked and information activities in a broader scheme of operations.

This chapter examines how operational command has manifest itself in the first two decades of the 2000s. It assesses the character of the operational dimension, reflecting on continuities and changes for commanders. It examines command and the complexity of the operational environment, command in the information environment, command and emerging technologies, command options in the information environment, decisive and shaping operations, and finally some reflections.

Command and complexity

The reason for the current 'crisis' is that the modern form of the operational dimension was designed to resolve a specific problem at a period in history when, on land, mass armies and improved communications were altering warfare profoundly. This epitome of operations, in industrial warfare, lasted well into the twentieth century. Naval operations were being transformed in the same period by developments in communications and the range of fires, but the chief concern was the handling of mass at sea, and its relationship to fire and manoeuvre. For air forces, the balance between manoeuvre in depth, fuel requirements, and the payload of fires or lift required its own doctrinal revolution. IOs were integral to all, but the balance of effect lay in the physical realm.

Since then, operational commanders have been compelled to consider a number of 'lines of operation'.[3] The commander has to incorporate different forces as a joint endeavour, liaise and co-operate with coalition partners, answer to political as well as military oversight, check intentions with legal advisors and political advisors, and sustain the momentum of the entire mission, while being contested by both overt enemies and more ambiguous adversaries. His or her staff will get tired, anxious, and sometimes make mistakes, while superiors will sometimes misunderstand or issue vague instructions which might be designed for interpretation as a 'broad intent'. Information management remains at the heart of these challenges, but the information environment is beginning to assert itself in new ways, with profound implications for operations.[4]

There are three areas where problems for commanders in the operational dimension present themselves: (1) greater complexity caused primarily by multiple, information-rich domains, axes, and lines of operation, (2) information and communications overload, and (3) the specific challenges of information and electronic warfare. These elements often overlap.

There are further challenges in the current grammar of war which have a bearing on commanders, including local proxies (such as the use of foreign militias or regular troops, an example being the appearance of Hezbollah units and Iranian troops in the conflicts in Syria and Iraq in 2014–2017); new or reintroduced weapons technologies designed to incapacitate or kill (such as nerve agent in urban operations in Syria, and Improvised Explosive Devices (IEDs) in Iraq); distributed and electronically enabled warfare at the tactical level (which enhances the fluidity of manoeuvre and fires); and the arms race in surveillance, encryption, and cyber-intelligence penetration (which could 'blind' an adversary and offer a brief window of opportunity for operational advantage).

It is equally complex when a multitude of different tasks might be required, from operational warfighting to peace-support. These often occur simultaneously, or within a short space of time and place. But complexity is not just in location and environment; it is also in the methods and systems employed. Recent conflicts against irregular actors indicate more 'distributed' warfare

where the enemy makes greater use of terrorism, a variety of stealthy tools, uses the civilian population as cover or for surveillance tasks, and, with extensive engagement of electronic media, makes maximum use of disinformation as the organ of propaganda and deception. In the conflicts of the 2010s, the enemies of the West had no significant air, counter-surveillance, or e-warfare assets. An adversary with near-peer capabilities would create far more serious difficulties, including greater damage, loss of air supremacy, and more significant attrition. Above all, one might also anticipate a far more sophisticated manipulation of the information environment.

Command and the information environment

Surveillance is a key element in the information age, enabling more precise targeting and a greater abundance of data for both physical and IOs. Improvements in technology have increased dependence on surveillance assets, command systems, and logistics, but also on their distribution. It is striking that irregular forces have often improvised their capability in surveillance, using proprietary hardware and software to create guidance for mortars and missiles, maximised use of surveillance footage for IOs, and made use of cheap drones to conduct Intelligence, Surveillance, and Reconnaissance (ISR) missions or IED strikes.

There is a dynamic 'arms race' of capability, countermeasures, and development in surveillance, concealment, and more generally in electronic warfare underway. This appears in the form of cyber and electro-magnetic activities (CEMA), but also as the search for stealth and more comprehensive surveillance. The concepts that are critical in the information space include penetration, protection, purging, (counter)penetration, and pursuit.

Intelligence-led operations and exploitation are critical in operations, where the West's adversaries operate among local populations and manipulate the aversion to civilian casualties. Even when Western forces observed strict rules of engagement in air operations over Iraq and Syria, groups like Daesh were not above inventing scenarios where, having killed civilians themselves, they claimed, cynically, that these casualties were somehow the result of Western operations.[5]

Information has been used to mobilise populations, to demoralise an adversary, and to encourage allies and neutrals; it has been used to recruit, to articulate a cause, and to reinvigorate conviction after serious setbacks. Some of the most powerful and memorable examples of information warfare have occurred when nations faced severe adversity. Today, the anxiety is that there is greater oscillation in public sentiment (driven by social media and internet access), concern that information must be delivered to a wider and more diverse audience rather than a clearly defined, national one, and that 'information operation thresholds' (where the public tolerance of military action is exhausted resulting in calls for operations to cease) are being lowered.[6] Commanders have become familiar with the fickle nature of public sentiment in the information environment.

For operational commanders, there seem to be discernible limits in policy terms that are driven by the broadcast of accidental civilian casualties, by episodes of indiscipline by military personnel, and by local insurgency or terrorism. The anxiety of governments is less about foreign disapproval than domestic criticism by the public or the press. A more serious military and political consideration is the lengths activists are now prepared to go to discredit authorities and conduct disruption. It is clear that all military and government installations will be under a certain level of threat from domestic sabotage, violent protests may engulf law enforcement agencies, and governments will be eager to minimise the level of popular antagonism by diluting policy.

Some military personnel express grudging admiration for Russian IOs, which manipulate the truth, and sell narratives which are blatantly distorted, but which appeal to a public proud of their nation, hungry for news that their country is asserting itself, and which desires success. Yet, the alleged value of multiple messaging, ambiguity, and denial, practised by Russia over Ukraine in 2014, confers only a short-term advantage. The contradictions of Russian IOs have sacrificed strategic credibility in the longer term. It was self-evident that the 'green gentlemen' without identifying insignia who seized Crimea by force were Russian military personnel and their success was due to an absence of real resistance.[7] In Ukraine's Donbass, Russia's proxies were a liability. Moreover, Russian denials that its proxies had shot down civilian flight MH17 were absurdly unconvincing.

As a countermeasure, it would be far better to pursue, through anticipation, foresight, and preparation, a phased approach to IOs. This would match Russian attempts to exploit ambiguity as a substitute, or prelude, for military operations. Synchronisation of effort in the media 'battlespace' can be accorded the same emphasis as fires, with the equivalent evaluation and assessment of effect. It can discern which messages are of strategic value and how sources are protected. In the operational dimension, every physical action requires deliberate and prepared information campaigns, with cascading rapid and responsive messaging that makes maximum use of information tactics.

Command and emerging technology

The accelerating development of certain weapons technology (unmanned vehicles, more precise air-delivered ordnance, better co-ordination of sensors and intelligence, and increased volume of fire with greater accuracy than 'area weapons' of the past) is well-known. There are likely to be new materials and other synthetic tools, additive manufacturing, and developments in robotics, all of which may have a greater effect on operations in the coming decades, and one can foresee robotic systems being contested by improvised automated systems and other semi-autonomous tools, from air platforms to smart mines, guided munitions, and tracking devices. This will

increase the pressure to cross traditional boundaries and 'silos' of organisation, to synchronise, centralise, and combine command in the operational dimension. There is a risk, however, that these novel systems will prove a distraction from the more urgent requirements in the conduct of war, and the full integration of physical operations and IOs.

The opportunities of new technology are for more accurate, comprehensive, and precise intelligence of targets; the ability to manoeuvre across domains to bring an appropriate package of effects to bear; and the ability to deploy robotic weapons to confront enemies that would otherwise inflict unacceptable loss of life. Nevertheless, in the information domain, commanders are likely to be asked, repeatedly, prior to and during missions, how a particular use of force is likely to enhance one's own information advantage or diminish the enemy's messaging, and the overall effect of the use of force in each scenario.

In counter-insurgency campaigns, commanders found themselves struggling to understand fractured societies. There was an estimation that the population were the centre of gravity and the rather limited way in which planners had discussed only 'enemy forces' was transformed into 'population-centric' counter-insurgency. More emphasis was placed on understanding the population, or 'human terrain' as it was styled. Yet understanding divided populations can take years, especially when they are placed under the extraordinary circumstances of civil war or insurgency and consequently behave differently, move out of their usual areas of habitation, or participate in the conflict. Moreover, the experience of the population in a civil war is invariably one of low-level intimidation, periodic acts of terror, significant 'hedging', and decisions based on their 'human security' and collusion.[8] This raises a significant question about their importance as an apparent centre of gravity in countering insurgencies. The current Western notion of operating by, with, and through locals is sound, laudable, and often effective, but it is not fool proof. Local actors have their agendas and a coincidence of objectives is always conditional and time bound.[9] A far more effective method, than understanding who the enemy *are*, is to assess what they think and believe, and who leads them. The population was 'the prize' but the means to get there was information. Information was, perhaps, a more reliable centre of gravity, and was always most effective when targeted at key leaders.

The management of information ought to be treated with at least the same importance as the provision of combat logistics, and, perhaps, today regarded as having parity with combat itself. Treating information as a centre of gravity would have a profound effect on any approach to operations: missions are designed with specific messaging in mind, deception is elevated in importance, targeted actors are more comprehensively 'shaped' in order to expose entire networks, and fires are used to develop subsequent information exploitation opportunities. The failure of an enemy to command the information space or be able to 'read' the networks will increase their chances of defeat.

Nevertheless, the fighting in Iraq and Syria has not been 'information-led', but 'fires-led'. It would therefore be erroneous to argue that war has been reduced to a battle of algorithms or texts. There is an indication that wars ahead will combine 'stand-off' fires, close-quarter battles, *and* information warfare. The solution is therefore the effective and smooth combination of fires and information, enabled by a mastery of technology.

The key is synchronisation. Instead of linear or even simultaneous approaches to operational design, synchronous activity suggests that it is the blending of consecutive or concurrent actions, in time and space, with the pressures that can be exerted by the environment itself. For Western commanders, synchronisation of fires and information, while making use of the information environment's nature, is required to achieve effects against the critical points, which might involve multiple, parallel lines of operation by different agencies. It might require some reversible phasing, that is, the ability to move backwards and forwards on a line of operation without loss of purpose, perhaps scaling back on levels of kinetic force to demonstrate the ability to control a particular zone. Plans would obviously need to be inclusive of any operational partners, and very often the organisation to deliver the effect would need to be tailored to the mission, a situation that requires great flexibility and goodwill on all sides. For example, a Special Operation Forces (SOF) presence with a forward air and IO cell, working amongst local forces, with a fully developed sense of the potential offered by an information environment, might be all that is required to achieve an operational effect.[10]

In the operational dimension, there are still many continuities. In terms of functions, it is still necessary to identify, through a centre of gravity analysis, the critical points; it remains vital to initiate arranging and shaping operations (to disrupt, delay, mislead, and otherwise impose friction), to manoeuvre (including interference with enemy communications), to deploy fires (including 'information'), and to consider command, including the neutralisation of an enemy's command, control, and communications.

There are opportunities for commanders in the optimal use of IOs and the full integration of cyber as an offensive asset. The anticipated effects are of impaired communications, navigation, shortages, loss of situational awareness, an absence of energy sources, and impact on policy-makers' direction and confidence. There may also be tactical effects such as deception, loss of stealth, concealment, and targeting. Being able to impose these problems upon an enemy will continue to confer a useful operational advantage, regardless of the technologies in use.

The essence of CEMA, or 'netwar', is deep operations, and responsibility for these is more likely to rest at the theatre and strategic level. However, if it was possible to neutralise or temporarily harness enemy communications and command systems, this advantage would be delegated to operational commanders for exploitation. The most common use of CEMA is likely to be enhancing situational awareness rather than episodes of sabotage, although

there is little way of knowing what technologies and coding will emerge in the next few decades to be certain of that. At the very least, commanders will be able to decide whether to exploit the access to enemy systems, or to remain passive and observant, in order to develop the penetration still further.

What troubles operational commanders today is a battlespace that is more technologically demanding, that they are constrained by bureaucracy and political leaders, and with hierarchy in command potentially undermined by new, more democratised media. They are concerned that every action is likely to be scrutinised to a forensic degree. There is still uncertainty about the best way to synchronise IOs and cyber to overcome these problems and achieve the optimum effects in both the physical realm and the information environment. War has long been heading in this direction and the complaints are not new.

The management of greater volumes of data and information increases the demands on headquarters but, at the same time, the dense and highly scrutinised information environment means that thresholds of what is considered tolerable could disrupt and even halt operations. The industrial systems approach invariably used by the West for command and decision-making in a dynamic and fluid information environment seems unfit for all purposes. The acceleration of time caused by more abundant and faster communications presents a fresh range of challenges for the operational commander.

Command options in the information environment

For decades, operational commanders have straddled the need to coordinate multiple entities from a communications hub and the desire to be 'forward' to keep in touch with the tactical situation.[11] The problem of too much data means that it is imperative that commanders create divisions of labour to manage it all, devolve responsibility while retaining a synchronised matrix of effects, and, given the speed of events, consider automation and brevity to initiate all sequences of action.[12]

Greater levels of automation are often to be found in analysis and decision-making. Data processing, especially in intelligence, fire control, air operations, surveillance, and logistics, is well established. As human labour becomes more expensive per capita, higher levels of automation are to be expected. This has created 'human-machine teaming'. To navigate a warship or an aircraft is a combined effort between humans and electronic systems. To launch missiles or ensure the right rations are delivered on time at the right location are the humble results of humans directing algorithms embedded deep within the tools that militaries use.

For many decades technical specialists have become as vital as combat personnel, and the division between them has blurred progressively over time. Commanders will struggle to keep up if they insist on commanding larger formations in great detail – they will need to permit the full spate of

data flow, rather than insisting on consultation over minutiae. They need to maintain a field of view and devolve the fight to subordinates.[13] Smaller formations in the land environment are the most cohesive and the most flexible, so commanders will feed in resources or deploy a reserve, to a far more distributed, devolved, and disaggregated command system.[14]

In information warfare and cyber operations, decisive points may be distributed and new centres of gravity will emerge, perhaps as cascading attacks on sources of energy supply on which an entire apparatus of information and networking relies. The requirement to make attacks across whole networks as well as attacking certain nodes will be evident. Surprise and security may be as difficult to achieve at the strategic level as it has always been, but new electronic opportunities for deception seem clear. There will be a much more compelling requirement to operate deep in the enemy's electronic heartland. Air, maritime, and space still offer the best opportunity to acquire depth, but the electronic and information environment reaches a global constituency all the time.

Regaining the initiative will require an intelligence-led offensive posture, pursuing relentlessly into depth. E-surveillance and signal interdiction are the most promising areas, with rapid reaction forces able to move into neutralise networks, systematically and precisely. It requires the containment, management, or neutralisation of large numbers of mobilised populations who are dependent on e-tools for communications and effects. Control or effective contestation of the e-space is vital.

Senior leaders appear reluctant to delegate responsibility in the command of operations, preferring to retain authority and therefore ultimate accountability.[15] In a litigious and social-media saturated world, those in authority seem much more sceptical of 'initiative'. This, however, is a mistake. The fast-moving information domain lends itself far more to mission command. Subordinates require education in its practice and its limits, but the information environment moves at such a tempo that a controlling approach is certain to be too slow. What is missing is the confidence and knowledge of leaders about the information environment, and, consequently, the willingness to devolve, engage in cyberspace, or in the information (from mainstream to social media) battle space to contest narratives.

Decisive and shaping operations in an informational context

Two elements of operations in the NATO framework now demand consideration for their implications well beyond the battlefield: those that are 'decisive' and 'shaping'. These are often overlapping and can, of course, be mutually supporting. Shaping, the activity required to create the conditions for a decisive action, or perhaps, to set the conditions, the thinking and therefore the actions of actors, is a crucial aspect of operations, which may involve the build-up of resources, information messaging, off-balancing manoeuvres, strikes in depth, cyber disruption, or even the arrangement of forces to reinforce a diplomatic message. There is often reference to fixing

an enemy, which can mean either being physically deprived of options or a psychological situation. If an enemy feels they have a limited range of options, they may act prematurely, withdraw, or escalate. Crucially, they can be drawn into predictable lines of action, ready to be interdicted, defeated, or naturalised. This may also be achieved through deception as well as through shaping actions.

Moreover, shaping can just as easily equate to denial. It can mean the prevention of an enemy reaching their operational or strategic objectives. Surprise can be critical in this regard, as it forces the enemy to divert attention, time, and resources to tasks they had not foreseen. Each of these implies actions deep in the enemy's domains and information space.

The decisive engagements of the past are often the most studied, but they were the culmination of a campaign rather than single events in isolation. They take place, ideally, at the centre of gravity of an enemy, be that a location, a force, a logistical node or other key capabilities, an enemy mission, critical requirements, particular vulnerabilities, a leader or some other dependent fulcrum. In reality, most actions take place over time across an enemy network and resemble attrition. In the current operating environment, which is dependent on electronic communications, navigation, and precision guidance, critical points are more likely to be located deep in their electronic infrastructure. Decisive actions will still be rare but could be achieved by the systemic disruption, slowing, or destruction of nodes and networks. The misstep of an opponent and a fortuitous exploitation could still be enough to cause his critical failure.

Manoeuvre, a concept that offers the opportunity to avoid the consequences of attritional or annihilationist options, will remain important in the e-environment. Manoeuvre involves the ability to blend lethal force and non-lethal actions to shape an enemy's behaviour, sap their will to resist, and break their cohesion. This is done by changes to momentum, tempo, shock, surprise, and relentless pressure, each of which have options in the information space. The overriding consideration is to seize and retain the initiative so as to dictate events and actions to the enemy. There is a requirement to exploit a situation, where reserves, fresh assets, changed axes, or a sudden surge of tempo can unhinge an enemy's strength. Sustaining pressure requires careful planning and reconstitution to avoid the effects of culmination.[16]

Information warfare consists of a full appreciation and exploitation of the information domain as an interactive environment, and actions which shape, strike, and exploit not only enemy actors but some of the infrastructure, cognition, and actions in that information sphere. The information space consists of a variety of actors and elements which are not passive, but active.

Reflections on command in an information age

Since operational art is concerned with command, we should conclude with reflections on leadership in the operational dimension and information environment to evaluate what has changed and what has not. Ultimately,

war is fought in the 'minds of men', regardless of the tools they use. The mind is subject to physical threats and opportunities, but information is its currency. The traditional observations about command functions and principles still stand despite changes in the character of war, but it is worth noting some new considerations that the information age has highlighted. The speed and tempo of operations mean that it is even to devolve responsibilities. The requirement to rapidly switch axes or domains means a commander must have familiarity with the various arms and branches of their force, including the cyber-electro-magnetic one. But of all the qualities commanders must possess, creativity is likely to be more important than formerly assumed. The operational environment will change rapidly, not least as the enemy adapts, and a commander too wedded to the approaches learned in staff college will rapidly lose touch with a situation. Creativity and devolution take courage, will invite criticism and increase demands, but it is surest way to an adaptive force.

Operations were formerly, and to some extent still are, shaped by the deprivation of the body of the enemy. Imposing burdens upon him were designed to create attrition and reduce his willingness to continue resistance. But the psychological element could be achieved without having to affect the body and the e-environment has offered new routes to that end. The combination of physical *and* e-enabled measures increases geometrically that effect.

It is clear that operational commanders need to manoeuvre in both physical space *and* the information environment, using a range of options, from high-intensity combat operations and IOs through to security or support missions, to 'shape' particular actors and contribute to certain objectives. By integrating capabilities, selectively or comprehensively, and synchronising actions and blending those with the opportunities afforded by the information domain, commanders will be able to concentrate on the most important aspect – the fulfilment of outcomes.

The savagery and devastation of a new era of weapons systems will demand the attention of military personnel. More importantly, they will need to acknowledge that the public will be the target in future conflict. This will undoubtedly take the form of low-intensity terrorism, mass casualty events, attacks on food security, energy, and information sources. The e-threat will be an increasingly significant part of the operational dimension and associated command problem for the armed forces as well as civilian authorities.

Operational commanders have more opportunities in the e-environment to create effects and to impose psychological and physical burdens on their adversaries. There is the prospect of harnessing the e-advantages of Western personnel, not least in the skill sets of computing, engineering, and analysis. There is the chance to operate in much greater depth than before and to secure advantages over an enemy, often long before the point of physical contact. But synchronised information and physical operations are now the norm.

Notes

1 Alexander Mattelaer, 'The Crisis in Operational Art', *European Security and Defence Forum Workshop 2* (11 November 2009).
2 US Army, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century* (Leavenworth, WA: US Army, 2017), https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf (Accessed June 2020).
3 DCDC, *Joint Doctrine Publication 003, Campaign Execution* (Shrivenham, 2012), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43329/20120829jdp300_ed3_ch1.pdf; Patrick Bury, 'Implications of Multi-Domain Battle: Welcome to the Jungle', *Wavell Room*, 19 September 2017, https://wavellroom.com/2017/09/19/welcome-to-the-jungle/.
4 Rudra Chaudhuri, Theo Farrell, 'Campaign Disconnect: Operational Progress and Strategic Obstacles in Afghanistan, 2009–2011', *International Affairs* 87:2 (2011), 271–296, Regis Debray, *Revolution in the Revolution* (New York: Grove Press, 1967).
5 For an example of Russian propagandists' exploitation of this allegation, see Anonymous, 'Mosul Airstrikes: US Seeks to "Shift Blame" for Civilian Casualties', *Sputnik*, 26 March 2017, https://sputniknews.com/middleeast/201703261051979557-mosul-airstrikes-us-civilian-casualties/ (Accessed March 2020).
6 See the Stanford review, Anya Schiffrin and Ethan Zuckerman, 'Can We Measure Media Impact? Surveying the Field', *SSIR* (Fall, 2015), https://ssir.org/articles/entry/can_we_measure_media_impact_surveying_the_field, for alternative perspectives see, Douglas Yeung, Sara Beth Elson, Parisa Roshan, S.R. Bohandy, and Alireza Nader, 'Can Social Media Help Analyze Public Opinion? A Case Study of Iranian Public Opinion After the 2009 Election', Research Brief (2012), https://www.rand.org/pubs/research_briefs/RB9685/index1.html (Accessed June 2020).
7 Janne Matlary and Tormod Heier, eds., *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe* (New York: Palgrave, 2016), ch.1.
8 Stathis Kalyvas, *The Logic of Violence in Civil War* (Cambridge: Cambridge University Press, 2006).
9 Rob Johnson, *Staying True to Their Salt: Partnering Local Forces* (London: Hurst & Co.: 2017).
10 Al-Ghaud radio, established by civilians under the occupation of Daesh in Mosul, is an example of this exploitation of the information environment. The clandestine radio exploited dissatisfaction with the Daesh occupation. Coalition forces supported the local initiative. Michael Stevens, correspondence with the author, December 2017.
11 See Howard Altman, 'Army's McMaster Talks about the Human Domain of War at USF Conference', *Tampa Bay Times*, 7 April 2015, http://www.tbo.com/list/military-news/armys-mcmaster-talks-about-the-human-domain-of-war-at-usf-conference-20150407/ (Accessed March 2020).
12 Land Warfare Development Centre, *Army Doctrine Publication Land Operations* (Warminster: Land Warfare Development Centre, 2017), 8–11.
13 Eitan Shamir, *Transforming Command: The Pursuit of Mission Command in the U.S., British, and Israeli Armies* (Stanford University Press, 2011).
14 Joe Strange, *Centers of Gravity & Critical Vulnerabilities: Building on the Clausewitzian Foundation So That We Can All Speak the Same Language*, *Perspectives on Warfighting* 4, 2nd edn. (Quantico, VA: Marine Corps Association, 1996).
15 Rickey E. Smith, 'Mission Command Current and Future', *Presentation*, 19 June 2013, http://www.dodccrp.org/events/18th_iccrts_2013/post_conference/plenary/smith.pdf (Accessed March 2020).

16 For example, Israel made extensive use of synchronised information and physical actions in its operations against Hamas in 2009. Israeli Defence Forces, 'IDF Begins Widespread Campaign on Terror Targets in the Gaza Strip', *Israeli Defence Forces Blog*, 14 November 2012.

References

Altman, Howard, 'Army's McMaster Talks about the Human Domain of War at USF Conference', *Tampa Bay Times*, 7 April 2015, http://www.tbo.com/list/military-news/armys-mcmaster-talks-about-the-human-domain-of-war-at-usf-conference-20150407/ (Accessed March 2020).

Anonymous, 'Mosul Airstrikes: US Seeks to "Shift Blame" for Civilian Casualties', *Sputnik*, 26 March 2017, https://sputniknews.com/middleeast/201703261051979557-mosul-airstrikes-us-civilian-casualties/ (Accessed March 2020).

Bury, Patrick, 'Implications of Multi-Domain Battle: Welcome to the Jungle', Wavell Room, 19 September 2017, https://wavellroom.com/2017/09/19/welcome-to-the-jungle/ (Accessed March 2020).

DCDC, *Joint Doctrine Publication 003, Campaign Execution* (Shrivenham, 2012), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43329/20120829jdp300_ed3_ch1.pdf.

Debray, Regis, *Revolution in the Revolution* (New York: Grove Press, 1967).

Israeli Defence Forces, 'IDF Begins Widespread Campaign on Terror Targets in the Gaza Strip', *Israeli Defence Forces Blog*, 14 November 2012.

Johnson, Rob, *Staying True to Their Salt: Partnering Local Forces* (London: Hurst & Co.: 2017).

Kalyvas, Stathis, *The Logic of Violence in Civil War* (Cambridge: Cambridge University Press, 2006).

Land Warfare Development Centre, *Army Doctrine Publication Land Operations* (Warminster: Land Warfare Development Centre, 2017).

Matlary, Janne, and Heier, Tormod, eds., *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe* (New York: Palgrave, 2016).

Mattelaer, Alexander, 'The Crisis in Operational Art', *European Security and Defence Forum Workshop* 2 (11 November 2009).

Schiffrin, Anya, and Zuckerman, Ethan, 'Can We Measure Media Impact? Surveying the Field', *SSIR* (Fall, 2015) at https://ssir.org/articles/entry/can_we_measure_media_impact_surveying_the_field.

Shamir, Eitan, *Transforming Command: The Pursuit of Mission Command in the U.S., British, and Israeli Armies* (Stanford University Press, 2011).

Smith, Rickey, E., 'Mission Command Current and Future', *Presentation*, 19 Jun 2013 http://www.dodccrp.org/events/18th_iccrts_2013/post_conference/plenary/smith.pdf (Accessed March 2020).

Strange, Joe, *Centers of Gravity & Critical Vulnerabilities: Building on the Clausewitzian Foundation so that We Can All Speak the Same Language*, *Perspectives on Warfighting* 4, 2nd edition. (Quantico, VA.: Marine Corps Association, 1996).

US Army, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century* (Leavenworth, WA: US Army, 2017), https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf (Accessed June 2020).

Yeung, D., Elson, S.B., Roshan, P., Bohandy, S.R., and Nader, A., 'Can Social Media Help Analyze Public Opinion? A Case Study of Iranian Public Opinion After the 2009 Election', *Research Brief* (2012), https://www.rand.org/pubs/research_briefs/RB9685/index1.html (Accessed March 2020).

18 The emotions of adversarial interaction

Lukas Milevski

Introduction

It has long been acknowledged that the human element of war is a primary source of its enduring nature. With his wondrous trinity, Clausewitz asserted that war is always dominated by the three forces of emotion or passion, reason, and chance, each in varying measure according to the specific circumstance of any particular war. These reflect the constraints of war's human dimension: we experience emotion; we seek to reason, partly on the basis of emotion; and we act in an environment rife with chance. Clausewitz further stipulated that '[o]ur task … is to develop a theory that maintains a balance between these three tendencies, like an object suspended between three magnets'.[1] Often, however, the emotional thread in strategy is lost in modern strategic studies scholarship and so theory is unbalanced in favour of emphasising reason and rationality. This is understandable – it is exceedingly difficult to study emotions – but a vital element in strategic theory is missing nonetheless.

Yet even while hampered by the as yet undeveloped state of psychology, Clausewitz repeatedly emphasised the importance of moral factors as well as the mental, including emotional, life of the commander in war. 'With our slight scientific knowledge we have no business to go further into that obscure field; it is important nonetheless to note the ways in which these various psychological combinations can affect military activity'.[2] In the approximately 200 years since Clausewitz, psychology and cognitive sciences have developed substantially. The human mind, while still wondrous and holding many mysteries, is no longer nearly wholly obscured as it was in Clausewitz's day. Instead, cognitive science and psychology have substantially developed as fields and their insights may be applied to the study of war and strategy. The key to relating this knowledge to strategy, particularly through the Clausewitzian trinity's frequently but usually superficially invoked emotional side, is understanding adversariality.

Adversariality underpins war. It is the key which starts war, a frame of mind in which interaction with the other party appears to be zero-sum, whether or not it actually is. There is a symmetry to adversariality: if evolving adversariality is one of the initiating phases leading to war, then

breaking that adversariality must similarly be one of the early developments leading to peace – the whole point of strategy in practice. In this chapter, the nature of adversarial relationships is explored in terms of both reason and especially emotion. Stress, emotion causation, and emotion consequences, especially fear, anger, and hope, are highlighted as being of particular relevance to developing our emotional understanding of strategy.

On adversariality

Clausewitz defines war as 'an act of force to compel our enemy to do our will'.[3] This elegant definition encompasses war's three fundamental elements: violence ('an act of force'), instrumentality ('to do our will'), and, most important for our purposes, adversariality ('compel our enemy'). Each element describes a different but necessary aspect of war. Violence and instrumentality have long received attention in the literature, but our understanding of adversariality, despite its definitional centrality to war, is still lacking. Many definitions of strategy tend to focus most on instrumentality, with violence in second place and adversariality distinctly third. Although adversariality is one of the most vital elements of war, one of the eternal threads which relate every war to every other war and define war as a phenomenon, it has hardly been studied and is not well understood.

Clausewitz's trinity posits that war is always beset by factors

> composed of primordial violence, hatred, and enmity, … to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone.[4]

When discussing adversariality as both a frame of mind and a description of mutual interaction between strategic actors one may disregard chance and probability. The standard Western supposition, a Cold War legacy, implies that the remaining two elements of the trinity are at odds: reason exists to control passion in war, to prevent escalation that might conceivably lead to Armageddon. Thus passion is adversarial and reason is instrumental. In *Clausewitz's Timeless Trinity*, for example, Colin Fleming adopts this perspective, that passion is equated to hostility, leaving reason free to deal with the difficulties of reconciling politics and policy in war.[5]

Yet Clausewitz distinguished between two different hostilities: hostile *feelings* and hostile *intentions*. Fleming suggests that both belong to passion, redefined simply as hostility.[6] This is inapt. Hostile feelings are clearly passionate and emotional, but Clausewitz differentiates between them and intentions:

> Essentially combat is an expression of *hostile feelings*. But in large-scale combat that we call war hostile feelings often have become merely

> hostile *intentions*. At any rate there are usually no hostile feelings between individuals. Yet such emotions can never be completely absent from war.[7]

Clausewitz defines hostile feelings as emotions, but implicitly categorises hostile intentions otherwise, as the product of reason. They represent intentionality about changing the future in the face of an actively resisting enemy and make adversariality as a whole a complex phenomenon to which both passion and reason contribute, albeit not necessarily in the same ways, at the same times, or with the same effects on strategy or the politics surrounding the war.

Adversariality in any particular belligerent context has its own life cycle: a beginning, a middle, and an end, with passion and reason engaged variously throughout the cycle. This cycle is born of politics, the basic context of war, a (usually) deliberate choice to employ armed force and so to practice strategy. The deterioration of any political relationship to the point of war both reflects an increasingly adversarial thread in that relationship and is simultaneously exacerbated by that thread. A characteristic of escalating adversariality is an increasing preference to resolve a political dispute using force, largely through the judgement that no satisfying outcome can be achieved with any means short of violence. Goals appear, rightly or wrongly, to be zero-sum and indivisible, the winner taking all. This is adversarial reasoning in the war's political context. By introducing violence, adversariality gets locked into the relationship, along purely emotional as well as reasoned trajectories.[8] As Clausewitz noted,

> [e]ven where there is no national hatred and no animosity to start with, the fighting itself will stir up hostile feelings: violence committed on superior orders will stir up the desire for revenge and retaliation against the perpetrator rather than against the powers that ordered the action.[9]

This is adversarial feeling, alongside which comes adversarial reasoning in strategy:

> So long as I have not overthrown my opponent I am bound to fear that he may overthrow me. Thus I am not in control: he dictates to me as much as I dictate to him…If you want to overcome your enemy you must match your effort against his power of resistance…But the enemy will do the same.[10]

Despite adversariality's natural tendency to escalate in war, ultimately the middle of the adversarial life cycle – battles and other engagements harbouring both adversarial feelings and intentions – is meant to bring adversariality to an end. The point of strategy is to employ force to create a situation in which violence, and strategy as such, become unnecessary

because the enemy's adversarial will has been broken and he has acceded to terms of some sort. That it is effectively self-negating when successful is a fundamental irony about strategy. Breaking adversarial will results in the enemy's changed belief and perception about the apparent zero-sum quality of mutual goals in the belligerents' relationship: the enemy is now willing to give up part or all of its war goals in return for peace. Just how do the cognitive sciences fit into the understanding of adversariality and the study of strategy in war?

Stress and emotion

Strategists navigating the dynamics of adversarial interaction in war do not just do so rationally but also 'irrationally' – emotionally. The main relevant cognitive sciences here relate to emotions as well as to stress. Unfortunately, consistent definitions of emotions have not emerged as researchers have generally preferred formulating operational definitions of emotion over conceptual ones to define their research interests.[11] This is particularly the case as an experienced emotional episode may contain many components – cognitive, feeling, motivational, somatic, and motor – and researchers may prefer focusing on any of these components individually or in combination.[12] As far as strategy is concerned, the key components are cognitive, feeling, and motivational. Stress is a distinct body of literature within the cognitive sciences, one which had historically, substantially, and unfortunately emerged without reference to or relation with the emotions literature. Unlike emotions, stress has been defined fairly simply: 'the struggle to adapt to life' and is the product of a relationship between a person and his or her environment.[13] Stress clearly must be present as a dimension of adversariality as the relationship between any strategist and the hostile; reciprocally violent environment of war is difficult to navigate and to manipulate against an independent enemy.

At the heart of both stress and emotion is *appraisal*, a specific term from emotion sciences which has gained ground to denote a particular cognitive approach to emotion. Appraisal theories are not the only theories of emotion, but they are usually the most relevant for strategy. Appraisal fits the agential orientation of strategy as a concept. 'The notion underlying appraisal theory is that personal evaluations of events – rather than the situations themselves – are crucially important in both eliciting and differentiating emotions'.[14] The act of appraisal by an active agent is key, and is also why emotions and their impact on decisions and behaviour sometimes seem so unrealistic to external observers. Appraisal also means that stress and emotions, in both causation and consequence, are particular to individuals.[15] Stephen Rosen's early attempt at incorporating cognition and neuroscience into the study of war and its termination is expanded below through discussions of stress and of the causation and consequences of emotions.

Stress

Rosen presents a simple thesis of how stress influences strategy: defeat in battle leads to the accumulation of distress among the defeated. Distress

> induces a condition very similar, and perhaps identical, to the psychological and physiological state of depression. Depression is defined symptomatically in terms of pessimism about the outcome of one's actions, lack of energy to perform tasks, and, in extreme cases, a collapse into near complete inaction.[16]

He suggests that this psychological process begins earliest with both the physical participants of battle and non-civilian elites, and that distress is contagious once it sets into an army. This leads to mass behaviour with which decision-making elites must contend in determining subsequent policy and strategy. One of the major elements Rosen identifies as contributing to distress, the primary reason why it sets in among frontline soldiers first, is uncertainty about the future and the individual's ability to control the environment. 'It is the losing side in a war that is subject to stressors in the environment that cannot be predicted or controlled'.[17]

Rosen's early thesis suffers from three main shortcomings. First, his focus is on stress with no mention of emotions other than those describing the parallels between distress and depression. This is an unfortunate reflection of the scientific literature itself, in which stress and emotions as concepts have traditionally developed independently of one another.[18] Yet stress influences emotions and tends to engender certain emotions over others. Second, his discussion of stressors focuses on battle as an experience, with an overly simple differentiation of battle understood as victory or defeat, excluding how other factors combine with and qualify outcome to determine the meaning of battle.

Third, Rosen focused on a lower level of analysis: that of individuals and groups of soldiers and officers, direct participants of actual battle, rather than strategists and certain policymakers. Clausewitz also worked with this lower level of analysis, as he described the feeling of defeat – which he had directly experienced after the battle of Auerstedt and throughout the ensuing French pursuit of the Prussian army across Prussia itself.

> When one is losing, the first thing that strikes one's imagination, and indeed one's intellect, is the melting away of numbers. This is followed by a loss of ground... Next comes the break-up of the original line of battle, the confusion of units, and the dangers inherent in the retreat... Then comes the retreat itself, usually begun in darkness, [and] continued through the night. Once that begins, you have to leave stragglers and a mass of exhausted men behind; among them generally the bravest – those who have ventured out farthest or held out longest. The feeling of having been defeated, which on the field of battle had struck only the senior officers, now runs through the ranks down to the very privates.[19]

Clausewitz described the effect of defeat on the conduct of strategy:

> The effect of all this outside the army – on the people and on the government – is a sudden collapse of the most anxious expectations, and a complete crushing of self-confidence. This leaves a vacuum that is filled by a corrosively expanding fear which completes the paralysis.[20]

Rosen was unable to relate these emotions back to the question of the strategist's agency; all he could say in concluding that theme is that '[t]he behavior of defeated troops in battle is not irrelevant'.[21] Although this is true, it remains unsatisfying nonetheless.

Stress is induced by any change in the environment, positive or negative, to which one must adapt, although clearly negative changes tend to create more stress. Scale matters as well: larger changes create more stress.[22] Stress emerges when an individual's resources appear insufficient to allow adaptation to environmental change. Crucially, stress is inherently relational: changes to the environment mean nothing if they are not relevant to individuals within it.

> A person is under stress only if what happens defeats or endangers important goal commitment and situational intentions, or violates highly valued expectations. The degree of stress is, in part, linked with how strong these goal commitments are, and partly with beliefs and the expectations they create, which can be realized or violated.[23]

Although stress may be – and has been – classified in a number of ways, one may suggest three various types of stress.

> *Harm/loss* deals with damage or loss that has already taken place. *Threat* has to do with harm or loss that has not yet occurred, but is possible or likely in the near future. *Challenge* consists of the sensibility that, although difficulties stand in the way of gain, they can be overcome with verve, persistence, and self-confidence.[24]

The act of appraisal is fundamental to stress: appraising changes in the environment and their relationship to oneself, appraising the quality of the changes (as positive or negative), appraising potential responses to the changes (is it possible to adapt to the change or not).

Furthermore, stress may accumulate if stressors in the environment propagate, whether laterally (new stressors appearing) or sequentially (existing stressors are exacerbated or grow in importance and/or proximity), without effective responses. As stress accumulates, that is, as it appears increasingly unlikely that one's resources or powers are sufficient to manage or adapt to changes in the environment, it becomes more difficult to regulate emotional responses to those or subsequent changes. The various types of stress may

engender related emotions, whether fear, anger, hope, relief, depending on specific outcomes or concerns about the future. Increased stress similarly increases the chances of feeling any given relevant stress emotion, and increases the intensity of that emotion.

Emotion causation

Consideration of emotions has been increasingly incorporated into international relations, culminating recently in a strong attempt to begin creating a theory of emotional choice in coercive diplomacy.[25] This has also filtered into strategic studies with similar work on the role of emotions in choice and decision-making in strategy, particularly relating to deterrence and war termination.[26]

Yet focusing on decisions is insufficient for strategic studies, as strategy is inherently more than mere decision-making. Without subsequent tactical, operational, and strategic performance, decision-making alone loses meaning; strategy requires a broader and more flexible understanding of emotion.[27] First, emotions must be contextualised in a longer performative process than isolated moments of decision-making. This leads directly to the second point, that emotion *causation* is equally important to emotion *consequence*. On-going strategic performance causes emotions in both adversaries, and those emotions have consequences for subsequent performance, which, in turn, causes further emotional reactions. Finally, this longer performative process, in which emotion causation and consequence are equally important, occurs within a specific range of violent and adversarial contexts and circumstances which often inhibit the full range of human emotion. Only some emotions are necessarily relevant to strategy or the strategist, although one must recognise that both context and level of analysis play a part. A strategist seems unlikely to commit to battle merely to bolster pride, but he may commit to battle because he is proud or, conversely, he may not cooperate effectively with a fellow commander in battle because he is (or they both are) too proud to do so.

Unless aiming for complete annihilation and conquest, the strategist inherently seeks to induce a psychological effect in the enemy which involves an emotional dimension. Understanding emotion causation, particularly in the adversarial context of war, is crucial. While myriad theories consider the question of emotion causation, appraisal theories focus on the act of appraisal in causing emotion. This act tends to centre on a few variables. One is goal relevance, or the relevance of a perceived change in the environment to one's ability to attain a currently held goal. Goal relevance also affects the intensity of emotions. Second is goal congruence, or the degree to which the perceived change in the environment helps or hinders goal attainment. Whereas goal relevance determines whether an emotion is felt, goal congruence determines whether that emotion is positive or negative. Beyond these two fundamental appraisal variables, various appraisal theories focus

on a variety of other possible variables, including level of certainty, potential to cope with the change, and the question of another's agency behind said change.[28]

Goals are related to another important consideration of appraisal theories: the issue of belief. Goals are held because they are believed to be attainable; if a goal were not attainable, there would be no sense in holding it.[29] This suggests that a change in the environment which elicits an emotional response also inherently affects, positively or negatively, one's beliefs or expectations about goal attainability. An emotional experience may imply an inherent revision of beliefs or expectations, particularly about the attainability of goals.[30] Yet this is not necessarily the case, as emotions may prevail despite rational appraisal that there is no meaningful change to the environment.[31] For example, one may still fear the height of the tower one has just climbed even while rationally knowing that the tower is architecturally sound and cannot collapse. Emotions may contain a substantial *denial* component; the person denies perceived reality in favour of a half-perceived, half-emotionally imagined reality. Expectations may be stronger than perceptions of environmental change.

Discussing emotions as inducers of belief revision implies that the need to revise was broadly unexpected. This observation seems not to have been explicitly made in the emotion sciences literature. If one expects an environmental change to revise one's beliefs, those beliefs have already been revised rather than waiting for the event to occur. Although it is too strong to say that surprise is inherent in any emotion – as one may still feel some emotions even if the situation develops along a desired or anticipated path – it is fair to suggest that the greater the deviation between expectations and results, the stronger the emotional response. This is important when tying emotion causation concretely with battle, which are not emotionally equal. If one engages in battle without serious hope of victory because the circumstances demand it – a rearguard action to cover a retreat, for example – battlefield defeat will not induce substantial negative emotions because defeat was expected and beliefs/expectations were already suitably revised (although it may still increase stress). In the context of strategy, therefore, strategically meaningful emotions seem most likely to occur when the environmental change is unanticipated, a surprise. Then-Commander James B. Stockdale, a prisoner in Hanoi during the Linebacker 2 bombings, observed this firsthand.

> Night after night the planes kept coming in—and night after night the SAM's streaking through the sky were fewer and fewer (the naval blockade worked). The *shock* was there – the *commitment* was there – and the *enemy's will was broken*. You could see it in every Vietnamese face. They knew they lived through last night, but they also knew that if our forces moved their bomb line over a few thousand yards they wouldn't live through tonight.[32]

The North Vietnamese had lived through quite a few US air raids by December 1972 and had become quite blasé about them, but the experience of Linebacker 2 was qualitatively different from any previous bombing campaign. North Vietnamese expectations were not in line with the reality the United States created – and the basis of North Vietnamese fear was surprise. Spurred by surprise and fear, the North Vietnamese returned to the negotiating table. Emotions are generated by unexpected environmental changes and individual appraisals of those changes, including whether they are relevant, positive or negative, and whether the individual can live with, or seeks to deny, those changes.

Emotion consequence

Although written with a focus on international relations decision-making, Markwica's summary of emotion consequences remains apt and useful for war termination. As discussed, emotions affect both cognition and behaviour. These effects are achieved through each emotion's own specific 'appraisal tendencies' and 'action tendencies'. Emotional influence on appraisal tendencies suggests that current emotions affect current or near future appraisals, which, in turn, feed into future emotions and emotional change or continuity. Action tendencies determine the likely range of behaviour stemming from a particular emotion. Ultimately, these are only *tendencies* and individuals do have considerable, albeit incomplete, control over how their emotions affect their subsequent actions. Markwica focused on five emotions in coercive diplomacy: fear, anger, hope, pride, and humiliation.[33] Concerning the emotional effects of *battle*, however, it seems useful to focus on three emotions: hope, fear, anger – which may also be considered part of the more complex emotional state of depression, which also includes anxiety, guilt, and shame. Unlike diplomacy, battle takes place in the adversarial setting of war. Considerations such as offending pride or humiliating the enemy become meaningful once the two sides start talking, but prior to the adversarial will being broken those specific emotions are less relevant.

Fear is a potential emotional reaction to perceived threats. Its appraisal tendencies include: hyper-vigilance towards the environment to detect current as well as potential other threats, which may as a by-product amplify the emotional experience of fear; inhibition of complex cognitive tasks which may interfere with that hyper-vigilance, but which also leads to less mental flexibility; and environment appraisal which stresses the apparently low level of certainty and low ability to control.[34] Fear is typically considered to have three main action tendencies: fight, flee, or freeze. These are self-explanatory: if one is afraid of a threat, one may decide to fight it or flee from it. Freezing is slightly ironic as an action tendency because its essence is in *not* acting – that is, being overwhelmed and cognitively shutting down. In war, at least on the battlefield, '[b]iologists and military analysts are now fairly certain that freezing is a more common response than either fighting

or fleeing'.[35] The individual experience of combat, with threats plausibly emerging in quick succession from many directions, can easily overwhelm one's senses and cognition, resulting in temporary but effective paralysis. Yet military analysts sometimes add one more response to fear which remains as relevant to the command of armies as to the individual soldier on the battlefield: *fussing*, or engaging in manageable tasks which do not directly involve engaging the enemy, the source of danger. These are tasks such as assisting crew-served weapons and carrying ammunition: 'simple jobs that a man can do instead of the really hard job he is supposed to be doing'.[36] Unlike the three classic F responses, fussing may be characterised as an oblique denial of the danger; yet it can nonetheless affect strategy and strategic performance.

Anger may arise from any number of potential appraisals, but most relevant for strategy is when another party blocks the achievement of an actor's goals. The main appraisal tendencies springing from anger include increased confidence in (re)gaining control of a situation; more optimistic risk assessments and minimisation of potential negative futures; and activation of heuristic processing resulting in less attention focused on quality of arguments and more on superficial cues. Anger's primary action tendency is to confront and attempt to remove or defeat the source of the anger.[37] Anger is an important element of depression, which has been described as:

> the result of a sense of hopelessness about restoring a worthwhile life following major loss. While being emotional, it is not a single emotion but a complex emotional state, a mixture of several emotions that come and go depending on where one is in the process of grieving and what has happened to produce the loss. The emotions of depression consist of anxiety, anger, guilt and shame. These are the emotions of struggle against one's fate because we have not yet given up on changing it.[38]

Besides anger, anxiety is a state of heightened concern regarding an uncertain future; guilt is experienced for transgressing some identified imperative; and shame is felt when one is unable to live up to some identified ideal. Often, guilt is associated with behaviour – guilty of failing to do something expected – while shame is associated with being – being someone who cannot achieve that thing. Guilt is thought to increase empathy with others, whereas shame may result either in the deterioration of social relations as blame for failure is externalised, or, conversely, in self-improving behaviour.[39]

Unlike fear and anger, hope is a positive emotion which arises from a desire to achieve a particular goal and a belief that achievement is possible. The appraisal tendencies associated with hope involve the facilitation of creative and imaginative instrumental thinking and cognitive flexibility but, more negatively, also a selection bias in perceiving the world in such a way as to sustain hope despite potential contradictory information. The action

tendencies associated with hope involve strengthening one's willpower and energy to act to achieve the desired goal. The selective perception tendency of hope may also feature as an action tendency, as hope may lead to conscious or subconscious information filtering.[40] Interestingly, hope is often considered to have a darker undercurrent due to its context and is experienced 'most often under an unfavorable situation. It is not clear whether hope is more often linked to negative life conditions than to positive ones'.[41]

Integrating strategy and emotion sciences

The insights gleaned from explorations of stress and the emotions must be properly integrated into Clausewitzian thinking and our understanding of strategic performance. One conclusion which immediately emerges is that Clausewitz basically got it right even by today's standards of modern cognitive science, albeit without the modern level of detail and awareness. Battle and warfare have, do, and will always stir up emotions on both sides of the battlefield. The unavoidable presence of such emotions will affect, positively or negatively, the difficulty of the strategist's task of breaking his enemy's adversarial will.

A strong strategic performance may inspire fear in the enemy, which is the desired emotional effect since most fright responses benefit the strategist. Freezing inhibits the enemy, fleeing weakens him, fussing distracts him. All three ease the strategist's task, both in the purely physical sense, that the enemy becomes easier to outfight later, and in the cognitive sense, that cracks begin forming in the enemy's adversarial way of thinking. Thus, instilling fear in the adversary may improve one's own future strategic performance relative to the enemy. However, fear may also lead to a fighting response, which reinforces the enemy's adversarial mindset and so increases the difficulty of the strategist's task.

Anger is usually not a desirable response as it generally leads to redoubled efforts by the opponent to win, unless the enemy's strategic performance born from anger can be channelled by stratagem in a way which actually disadvantages him. Nonetheless anger psychologically inhibits the strategist's task of breaking the enemy's adversarial will. Unless and until anger expends itself or is somehow excised, the effects of strategy on the enemy should perhaps be measured less in terms of psychological consequences and more in terms of physical ones. A possible exception is anger experienced as part of depression, when the adversary already feels that his situation is hopeless and experiences psychological breakdown, but is not willing to abandon efforts to improve his situation.

Hope may be the most strategically nuanced emotion of those discussed, as possibly the most sensitive to the outcomes of strategic performance, but also possibly simultaneously misleading. Hope can also inhibit the strategist's task of breaking the enemy's adversarial will. If the strategist himself feels hope, he may begin misinterpreting the facts on the ground to his own

ultimate detriment. If the enemy feels hope, it strengthens his adversarial will and makes it harder to break. Even in defeat, if the victor did not do as well as expected or the defeated lost less badly than expected, hope may arise again. (Conversely, despair may similarly arise among battlefield victors – one thinks of King Pyrrhus of Epirus whose three battlefield victories against Rome destroyed his army and along with it his ambitions for defeating Rome.)

Integrating emotion sciences with strategy and particularly with an appreciation of strategic performance can improve our understanding and deserves substantially more development, given the complex and nonlinear relationships between the two fields.

Conclusion

If the human element is truly the font of the most enduring dimensions of war, then one must be interested in the human experience of strategy. Such an interest must begin with an understanding of adversariality and the ways of thinking it both reflects and engenders. These ways of thinking necessarily include both stress and a panoply of emotions. Any strategy, in practice as well as in accounts of it, will always have an emotional aspect, including how it contributes to breaking the adversarial will of the enemy and ultimately to war termination. The emotional focus of strategy devolves onto fear, anger, hope, and onto stress and depression, this last a complex and fluid mixture of anger, fear, anxiety, guilt, and shame. The emotional tales inherent in strategy are myriad but too little understood and explored in a field whose understanding they can only enhance.

Notes

1 Carl von Clausewitz, *On War*, Michael Howard, Peter Paret, eds. and trans. (Princeton, NJ: Princeton University Press, 1984), 89.
2 Clausewitz, *On War*, 106.
3 Ibid., 75.
4 Ibid., 89.
5 Colin M. Fleming, *Clausewitz's Timeless Trinity: A Framework for Modern War* (Farnham: Ashgate, 2013), 57–70.
6 Ibid., 62.
7 Clausewitz, *On War*, 137.
8 On beginning adversariality, see Lukas Milevski, 'Choosing Strategy: Meaning, Significance, Context', *Infinity Journal* 6:2 (2018), 12–16.
9 Clausewitz, *On War*, 138.
10 Ibid., 77.
11 Carroll E. Izard, 'The Many Meanings/Aspects of Emotion: Definitions, Functions, Activation, Regulation', *Emotion Review* 2:4 (2010), 363–370.
12 Agnes Moors, 'Theories of Emotion Causation: A Review', *Cognition and Emotion* 23:4 (2009), 626.
13 Richard S. Lazarus, *Stress and Emotion: A New Synthesis* (New York: Springer, 1999), 29.
14 Julian W. Fernando, Yoshihisa Kashima, and Simon M. Laham, 'Alternatives to the Fixed-set Model: A Review of Appraisal Models of Emotion', *Cognition and Emotion*

31:1 (2017), 19, see also Roger Giner-Sorolla, 'The Past Thirty Years of Emotion Research: Appraisal and Beyond', *Cognition and Emotion* 33:1 (2019), 48–54.
15 See for example Matthias Siemer, Iris Mauss, and James J. Gross, 'Same Situation – Different Emotions: How Appraisals Shape Our Emotions', *Emotion* 7:3 (2007), 592–600.
16 Stephen Peter Rosen, *War and Human Nature* (Princeton, NJ: Princeton University Press, 2005), 100.
17 Ibid., 113.
18 Lazarus, *Stress and Emotion*, 35.
19 Clausewitz, *On War*, 254.
20 Ibid., 255.
21 Rosen, *War and Human Nature*, 134.
22 Lazarus, *Stress and Emotion*, 51, 52.
23 Ibid., 60.
24 Ibid., 33.
25 Robin Markwica, *Emotional Choices: How the Logic of Affect Shapes Coercive Diplomacy* (Oxford: Oxford University Press, 2018).
26 See for example Keith B. Payne, 'Understanding Deterrence', *Comparative Strategy* 30:5 (2011), 393–427; Kenneth Payne, 'Fighting On: Emotion and Conflict Termination', *Cambridge Review of International Affairs* 28:3 (2015), 480–497.
27 On the performative aspect of strategy see Lukas Milevski, 'Western Strategy's Two Logics: Diverging Interpretations', *Journal of Strategic Studies*, https://doi.org/10.1080/01402390.2019.1672158.
28 Agnes Moors, 'Theories of Emotion Causation: A Review', *Cognition and Emotion* 23:4 (2009), 640.
29 See for example Gerald L. Clore, and Karen Gasper, 'Feeling Is Believing: Some Affective Influences on Belief', in Nico H. Frijda, Antony S.R. Manstead, and Sacha Bem eds., *Emotions and Beliefs: How Feelings Influence Thoughts* (Cambridge: Cambridge UP 2000), 10–44.
30 Pierre Livet, 'Emotions, Beliefs, and Revisions', *Emotion Review* 8:3 (2016), 240–249.
31 Sabine A. Döring, 'The Logic of Emotional Experience: Noninferentiality and the Problem of Conflict without Contradiction', *Emotion Review* 1:3 (2009), 240–247.
32 James B. Stockdale, quoted in U.S. Grant Sharp, *Strategy for Defeat: Vietnam in Retrospect* (San Rafael: Presidio Press 1978), 258.
33 Markwica, *Emotional Choices*, 7.
34 Ibid., 74.
35 Leo Murray, *Brains & Bullets: How Psychology Wins Wars* (London: Biteback Publishing, 2013), 90–91.
36 Ibid., 105.
37 Markwica, *Emotional Choices*, 75–76.
38 Lazarus, *Stress and Emotion*, 242–243.
39 Kristy K. Dean and Elizabeth H. Fles, 'The Effects of Independent and Interdependent Self-construals on Reactions to Transgressions: Distinguishing between Guilt and Shame', *Self and Identity* 15:1 (2016), 91.
40 Markwica, *Emotional Choices*, 78, 86–87.
41 Lazarus, *Stress and Emotion*, 241.

References

Afflerbach, Holger, and Strachan, Hew, eds., *How Fighting Ends: A History of Surrender* (Oxford: Oxford University Press, 2012).
Blainey, Geoffrey, *The Causes of War* (New York: The Free Press, 1988).

Clausewitz, Carl von, *On War*, Howard, Michael, Paret, Peter, eds. and trans. (Princeton, NJ: Princeton University Press, 1984).

Clore, Gerald L., and Gasper, Karen, 'Feeling Is Believing: Some Affective Influences on Belief', in Frijda, Nico H., Manstead, Antony S.R., Bem, Sacha, eds., *Emotions and Beliefs: How Feelings Influence Thoughts* (Cambridge: Cambridge University Press, 2000), 10–44.

Dean, Kristy K., and Fles, Elizabeth H., 'The Effects of Independent and Interdependent Self-construals on Reactions to Transgressions: Distinguishing between Guilt and Shame', *Self and Identity* 15:1 (2016), 90–106.

Döring, Sabine A., 'The Logic of Emotional Experience: Noninferentiality and the Problem of Conflict without Contradiction', *Emotion Review* 1:3 (2009), 240–247.

Fernando, Julian W., Kashima, Yoshihisa, and Laham, Simon M., 'Alternatives to the Fixed-set Model: A Review of Appraisal Models of Emotion', *Cognition and Emotion* 31:1 (2017), 19–32.

Fleming, Colin M., *Clausewitz's Timeless Trinity: A Framework for Modern War* (Farnham: Ashgate, 2013).

Gartner, Scott Sigmund, *Strategic Assessment in War* (New Haven, CT: Yale University Press, 1997).

Giner-Sorolla, Roger, 'The Past Thirty Years of Emotion Research: Appraisal and Beyond', *Cognition and Emotion* 33:1 (2019), 48–54.

Lazarus, Richard S., *Stress and Emotion: A New Synthesis* (New York: Springer, 1999).

Livet, Pierre, 'Emotions, Beliefs, and Revisions', *Emotion Review* 8:3 (2016), 240–249.

Markwica, Robin, *Emotional Choices: How the Logic of Affect Shapes Coercive Diplomacy*, (Oxford: Oxford University Press, 2018).

Milevski, Lukas, 'Choosing Strategy: Meaning, Significance, Context', *Infinity Journal* 6:2 (2018), 12–16.

Moors, Agnes. 'Theories of Emotion Causation: A Review', *Cognition and Emotion* 23:4 (2009), 625–662.

Murray, Leo, *Brains & Bullets: How Psychology Wins Wars* (London: Biteback Publishing, 2013).

Payne, Keith B., 'Understanding Deterrence', *Comparative Strategy* 30:5 (2011), 393–427.

Payne, Kenneth, 'Fighting on: Emotion and Conflict Termination', *Cambridge Review of International Affairs* 28:3 (2015), 480–497.

Reiter, Dan, *How Wars End* (Princeton, NJ: Princeton University Press, 2009).

Rosen, Stephen Peter, *War and Human Nature* (Princeton, NJ: Princeton University Press, 2005).

Sharp, U.S. Grant, *Strategy for Defeat: Vietnam in Retrospect* (San Rafael, CA: Presidio Press, 1978).

Siemer, Matthias, Mauss, Iris, and Gross, James J., 'Same Situation – Different Emotions: How Appraisals Shape Our Emotions', *Emotion* 7:3 (2007), 592–600.

Part VIII

Conclusion

Lessons for thinking about war

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

19 Conclusion

Assessing change and continuity in the character of war

Tim Sweijs, Rob Johnson and Martijn Kitzen

Every age has its own kind of war with its own peculiarities. War's nature may be enduring; its character is prone to change – in each era as well as in each encounter. Ours is a time of considerable, some argue accelerating, societal, economic, political, and technological change. Accelerating or not, this megatrend of change permeates almost all walks of human life: how we live and communicate, how we work and collaborate, how we interact and create, and, to a large degree, how we fight. It thus affects how we prepare, equip, and organise for war as well as how we conduct war. Contemporary war continues to be characterised by the three enduring elements of kinetic activity, connectivity, and the symbiotic relationship between the human and the synthetic. The overarching theme that emerges from the contributions to this volume is the fact that across all three elements there has been considerable change over the past two decades.

The democratisation of kinetic means, traditional and non-traditional

On the kinetic front, a key trend has been the dissipation of power and the democratisation of violence. Put simply, the Davids of this world stand a better chance against the Goliaths. Insurgencies are proving to be remarkably robust confronted with ostensibly superior firepower in various conflict zones around the world. Beyond any doubt, in the past Western armed forces often faced difficulties in the fight against non-state adversaries. Today's non-state actors, however, prove to be increasingly capable of challenging ostensibly much stronger powers. In the 2010s IS showed how violent groups are able to punch above their initially purported weight. IS' ruthless exploitation of synthetic and connected elements allowed it to generate kinetic effects at a regional and even global level, greatly enhancing its resilience to withstand external attacks. The perseverance of other groups such as Al-Qaeda, Al-Shabaab, and Boko Haram – which were all targeted in extensive military campaigns – illustrates the levelling of the playing field between violent state and violent non-state actors. In the context of renewed confrontation between major military powers, violent non-state actors also

serve as puppets and proxies in increased grey zone competition. Russia's ties to the Donbass People's Militia in Eastern Ukraine, Iran's Quds Force's orchestration of Hezbollah fighters in Iraq and Syria, Egypt's – as well as rich Gulf states' – support for Khalifa Haftar's Libyan National Army in Libya may well be harbingers of what the 2020s will bring.

This all concurs with a more general trend of a changing balance of power between major and lesser military powers. These now have military capabilities at their disposal that allow them to level the playing field in a way that was unthinkable only a generation ago. Advanced C4ISR as well as military standoff capabilities are no longer the prerogative of Western powers alone. Low and high tech unmanned (weapon) systems are starting to be deployed by many conflict actors in the air and on land. Western military powers may still enjoy tactical military dominance, but Western military supremacy is no longer. Tactical excellence and operational craftmanship notwithstanding, strategic proficiency has been in short supply for an extended period of time now. Political leaders, especially, have performed poorly when it comes to formulating clear but also realistic political objectives, and allocating the required means to achieve these objectives. Other state actors have arguably proven to be more agile and more adept, both in terms of their ability to set coherent strategic objectives, match these with the required means, and to follow through on them, and in terms of their ability to adapt and innovate. A general disinclination prevalent in Western polities to engage with the messy and bloody realities of war based on a declining willingness to fight in postmodern societies has been further fed by close to two decades of few strategic successes in missions that yielded even fewer tangible benefits. This, in combination with steady technological progress in unmanned systems since the early 2000s, has resulted in greater emphasis on a new form of risk management from above and from afar, typically in collaboration with local proxy actors and spearheaded by small contingents of special forces, giving another dimension to the function of security force assistance. Such forms of risk management, variously indicated with terms as remote, surrogate, or liquid warfare, have become more prevalent over the past period amidst increasing geopolitical tensions. They are replacing the emphasis on counterinsurgency (COIN) and stabilisation missions of the aughts. It is far from certain that the valuable lessons learned during these missions will not be forgotten in a repetition of the strategic amnesia of the lessons painstakingly learned from counterinsurgencies in the past.

The exploitation of novel forms of *kinesis*

Meanwhile, new forms of *kinesis* – means and ways to exert pressure – have progressively materialised. The global wiring of our world of the past quarter century has paved the way for unprecedented global connectivity, alongside introducing a range of economic and social opportunities but also critical vulnerabilities that soon started to be exploited for malign

purposes. The existence of these vulnerabilities was identified by futurists and by military professionals already in the 1990s. The 2000s saw cautious experimentation with incidental, some would say audacious, endeavours in the latter half of that decade. But it was not until the 2010s that these were followed up with more serious large scale development of capabilities, strategies, and tactics deployed in real world operations, which are now taking off. A number of high profile cyber operations on but certainly also off the battlefield with considerable strategic impact showcased to all participants the tactical and strategic effects, if also the risks and limitations, associated with action in this new domain. The deployment of cyber instruments, alone or in combination with kinetic instruments, is now increasingly becoming the norm. For every pundit that argues this is a brave new world, there is a traditionalist arguing precisely the opposite. Be that as it may, international legal scholars and practitioners see themselves forced to reflect on the reinterpretation and possible adjustment of the rules and regulations guiding behaviour *in bello*, *ad bello*, and *extra bello*.

Political warfare in a connected world

The virtual arteries traversing our digitally connected societies have opened up a cloud of new possibilities to exert influence in the information realm. Traditional tricks of the political warfare trade are being applied to great effect, albeit in thoroughly modernised guises. The viral nature of information flows in social networks is exploited by shrewd conflict actors. The battle of the narrative in conflict theatres has given way to the emergence of widespread meddling in societal discourses in peacetime. In hindsight, the CNN effect of the 1990s pales in comparison to the effects of manipulated messages flowing through billions of people's Facebook or Weibo feeds. The echoes of these social media chambers expose a much more vulnerable cauldron than most political scientists and sociologists anticipated prior to the widespread adoption of these platforms over the past decade. The manipulation of societal discourses is nothing new and has been practiced by Western and non-Western powers alike – long before it started to be amply documented during the Cold War. Its sheer scale and impact, however, have become a pernicious problem that all actors, regardless of their regime type, are grappling with. Military commanders and their political leaders must now, certainly more than before, consider how citizen journalists or hostile state actors report on military operations, and anticipate how information will be faked, tweaked, and manipulated by adversaries. In the early stages of a conflict or confrontation, disinformation is often used to seize the initiative in the battle for the narrative. When a conflict continues for an extended period of time, a general sense of fatigue with a particular cause can creep in. This may result in a wish to move on to other things. Accumulating effects are difficult to differentiate from fatigue with a particular cause, but it is becoming clear that being first with the truth, deploying mass

in the scale of messaging, and being determined to see things through can win or lose a key narrative.

The effect of new propagandistic means on the conduct of war itself is certainly non-negligible either. The manipulation of information has become part and parcel of military operations across the globe once again implying that the truth is the first casualty of war. Western and non-Western military organisations have set up entire information manoeuvre units to pro-actively shape the information sphere in recognition of their vital role in compelling adversaries to change their minds. Russia's endeavours on this front certainly inspired others to copy and imitate. But the success of non-state actors and their ability to rally support, recruit adherents, and attract finance certainly also played a role. Information operations expanded not just the reach of non-state actors in the virtual realm but also their sheer prowess to project power in the physical realm. IS' rise in the 2010s and its tenacious tenure before it was defeated, at least in its conventional force incarnation, provided concrete corroboration of the risks posed by decentralised, distributed networks.

The impact of legal lawfare

Meanwhile, the term legal lawfare has been coined to describe contemporary conflict behaviour. This represents conceptual over-stretch to some who hold that war in its essence is about the organised use of violence in pursuit of political goals. Yet, the extensive legal corpus guiding the conduct of war, which has been spun since the days of Cicero and has been adjusted but also strengthened especially since the early 20th century, is now used and abused by state and non-state actors, both outside but also within the more traditional notion of war. Outside war, state actors seek to remain below the threshold of war and refrain from declaring war, leading to the pervasiveness of so called hybrid conflict, grey zone confrontation, strategic coercion or, in a more recent designation, liminal warfare. Inside war, there is an increasing salience of conflict actors seeking to gain tactical and strategic advantage over their opponents that try and abide by the laws of war through the positioning of military assets in the proximity of civilian facilities to induce violations and through the framing and distribution of the news of real or fabricated violations through media channels.

Vicious dynamics of renewed great power confrontation

Amid all the confusion about the impact of new domains on war, and heated debate about the analytical value of new nomenclature to capture changes in its character, great power competition and conflict have re-emerged. Starting in the early 2010s, established – (United States), emerging – (China), and resurgent powers (Russia) embarked on large scale military modernisation programmes with other states following suit. These major powers

are since prioritising not just the refurbishment of their conventional military capabilities but also seek to gain incremental as well as a punctuated strategic-military edge through investment in potentially more disruptive or enabling technologies, including Artificial Intelligence (AI). They are gearing up for renewed peer competitor conflict with the renewal of their nuclear arsenals, a shift to more aggressive nuclear postures, the development and deployment of a new generation of hypersonic delivery vehicles, and renewed attention to the militarisation of space. Meanwhile, frequent military aerial intrusions of national sovereign airspaces as well as gunboat diplomacy have become a regular recurrence in major powers' attempts to carve out and reconfirm spheres of influence, which is further driving a vicious cycle of military competition that in the 2010s did not escalate into direct major power conflict.

Incremental change: Machine learning in military operations

On the synthetic front, the explosion of computing power and the development of hardware (coincidentally as a side effect of a booming global gaming industry which spurred progress in graphical processing units' power) paved the way for rapid advances in machine learning (ML) from 2011 onwards. Military organisations were certainly not amongst the early adaptors, but confronted with the tremendous value created in industries as varied as trading and investment, advertising, and medicine, they started stepping up their efforts in the second half of the 2010s. They formulated plans, allocated considerable budgets, and started experimenting with the integration of ML applications in standing operations including in monitoring and detection, target acquisition, navigation, and logistics. Thus far, this is leading to incremental progress predominantly through the faster processing and analysis of ever greater amounts of information. The constant flow of information through ubiquitous surveillance capabilities is forcing the adaptation of command and control structures. ML has furthermore boosted the navigation abilities of semi-autonomous systems, and has made the enormously complicated and costly logistics required for fielding modern armed forces more efficient. It is, albeit slowly, contributing to shorter OODA loops, along different elements of that chain, and promises to change the economics of force generation in the future.

The role of the synthetic – in reality, not in science fiction

Hyper war remains at the horizon for now, but *accelerated war* is already a reality. In that sense, the 2010s have shown us glimpses of what AI enabled war can look like. Images of a dystopian future in which robots have taken over remain science fiction for the time being, but early manifestations of AI enabled war are definitely visible. In that vein, All Domain Operations is still a future concept but joint operations, enabled increasingly by more

advanced technologies, are integral to contemporary warfare. Similarly, mosaic warfare is still being funded by the Defense Advanced Research Projects Agency (DARPA) as an aspirational concept, but networked and distributed warfare have become a reality. In sum, the aspirations of the 1990s of informationised war materialised in the 2010s, whereas the intelligentised battlefield as envisioned by the Chinese remains an aspiration to be imagineered in the decade(s) to come. Overall, the *synthetic* – the artificial and the manufactured – has been making further inroads into the ways in which violence is wielded in the pursuit of political objectives both as an enabler and as an effector. The synthetic has only done so, however, as an extension of the human, which continues to give it shape and direction, but the combination of the synthetic and the human is giving birth to new ways of war.[1] In other words, while synthetics greatly enhance the ability to deliver pressure, resist threats, and even command, it is the human who remains in control.

The development of new grammars for war

During this period of considerable change, strategists grapple with the adaptation of time tested strategic concepts to the challenges posed by today's conflict environment, and consider how 19th- and 20th-century strategic concepts such as centre of gravity and deterrence can be tweaked, expanded, and refined to be brought to bear in this domain. The heated debates are not only testament to the explosion of information exchange in a globally connected world. They are also emblematic of the fact that the grammar of war defined as the principles, rules, and procedures that govern the use of force in new domains, as well as how it can contribute to its overarching logic, is being reinvented.

The idea of a logic in war has long been contested, but in our current context, what is discernible is a renewed sense of the utility of armed force in the service of political objectives. E. H. Carr, the British historian, noted that it is always hard to perceive the major shifts in the period in which you are living. The sheer flux of events and changes often obscure the trends, and we are, to cite Hegel, always wise after the event. Many political scientists discern a decline in war which began in 1945, at the same time as many social scientists maintain that violent conflict has seeped down from states into societies. Strategic thinkers, meanwhile, are concerned that major conventional wars may not be obsolete at all, and they see all the indicators of more serious, high-intensity, extremely lethal struggles ahead.

The grammar of war, too, is difficult to nail down to a single essence or character. In the case of extremist groups like IS, its atrocities suggested an inclination for the application of overwhelming and unlimited force. Western militaries, by contrast, relied on air supremacy, aerial surveillance instruments, and precise weapon systems to limit their interventions to the least destructive possible without jeopardising their objectives. Russia and China have adopted different grammars of their own – using force as

leverage, intimidation, and the breaking of international norms, including the use of violent proxies. Which of these constitute the grammar or character of the early 21st century? The answer is surely that they all do: war is protean. Its form is certainly significant but so are its purpose and essence which in the end dictate its logic.

Change and continuity in the character of war

In the study of war, scholars tend to focus on the eternal and the constant, whereas futurists and technologists tend to focus on the transformational and the novel. The former tend to be of the opinion that the more changes, the more remains the same. The latter tend to find that radical change is always around the corner. The truth, perhaps, lies somewhere betwixt and between. Many overestimate the impact of the rate of change in the short term, but underestimate it in the longer term. However, when the future finally arrives, they quickly adjust, and accept the state of affairs as normative. This is simply because the many iterations and developments in war's conduct accumulate into the present. Philosophically, the future that was imagined back in the days of J.F.C. Fuller has happened. He maintained that the conduct of war could be understood as control, pressure, and resistance. Such a broad categorisation allowed him to incorporate a variety of developments, and yet still conceive of how a war could or would be conducted. We can be sure, as Fuller was, that wars will happen in the decades that lie ahead. Wars will be defined by setbacks and successes, by frustrating friction, by human failures, technological breakdowns as well as breakthroughs, and all that thousands of years of human history has informed us is unchanging in war's nature.

The conclusion of our volume is therefore that we should neither exaggerate the transformational changes in the character of war nor downplay the extent to which elements in the character of war have in fact changed, even if these were largely evolutionary rather than revolutionary. Certainly many aspects remain the same and endure: war continues to be about the organised use of violence in the pursuit of political objectives; it continues to generate the passions and emotions of people of flesh and blood; and it continues to be characterised by uncertainty and friction. The world of war, lest we forget, is expansive and diverse. Polities in different geographical regions find themselves along varying developmental trajectories which shapes why and how they wage their wars. Local level armed conflict over access to water and land in sub Sahara Africa contrasts with the internationalised intrastate conflicts over larger geopolitical interests in the Middle East. These are, in turn, distinct from Russia's war with Ukraine.

Our volume, we hope, has made clear that, over the past two decades, increased connectivity and the emergence of new synthetic elements have shaped old forms and created new forms of kinesis. This process has fundamentally impacted the way wars – both low tech and high tech and high

intensity and low intensity – are fought across the globe. In the context of these three elements our volume shows that war, in the first decades of the 21st century, continues to be a fundamentally political endeavour. Developments along the kinesis-connectivity-synthesis trinity provide a good baseline to understand likely future trajectories in how humans wage future wars.

Note

1 This is in line with the etymological origins of the term *arms* which strays back to the Proto-Indo-German root -Ar, which means 'to fit together', suggesting that *arms* can also be conceptualised as a way of joining the human with the artificial. That, in turn, can be etymologically associated with the roots of synthetic deriving from the Ancient Greek meaning of the term synthetikos (συνθετικός) which stands for a composition based on 'putting something together'. If nothing else, it illustrates that tools and technology depend on how they are put to use by humans.

Index

adaptation 6, 11, 27, 181, 191–198, 284, 299, 300
adversariality 279–282, 290
Afghanistan 3, 18, 19, 20, 22–25, 73, 74, 131–134, 140, 144, 146, 159, 176, 177, 179–182, 189–190, 191, 194–197, 212
air power 3, 12, 25, 45, 131–141, 142, 143, 145, 146, 151
appraisal 50, 224, 282, 284, 285–286, 287–289
artificial intelligence 3, 9–11, 12, 30, 72, 93–111, 124, 139, 299
autonomous weapons 94, 101, 106–108

behaviour 24, 47, 59, 69, 72–79, 82, 83, 119, 143, 145, 162, 178, 275, 283, 287–288, 297, 298

China 7, 29, 45, 48, 49, 50, 94, 108, 121, 123, 133, 139, 195, 249, 298, 300
command 6, 8–9, 10, 11, 51, 53, 62, 109, 133, 137, 138, 167, 192, 196, 225, 267–276, 288, 299, 300
communication (strategy) 27, 58–69, 74, 244, 258
connected 3, 5, 8–9, 11, 12, 14, 297–298, 300
control 5, 6, 8–9, 10, 11, 46, 49, 51, 58, 63, 65, 66, 68, 72–84, 95, 99, 107, 109, 110, 133, 137, 143, 147, 149, 150, 161–165, 169, 175, 212, 239, 253–254, 272, 274, 280, 281, 283, 287–288, 299, 300, 301
conventional warfare 49, 73, 181, 182, 195, 267
counter-insurgency (COIN) 6, 7, 19, 22, 23, 25, 27, 29, 72–73, 74, 82, 133–134, 137, 140, 166, 179, 181, 189–198, 250, 296
countermeasures 116–125, 269
counter-terrorism 18, 145
cyber operations 12, 47, 118, 119, 121, 125, 136, 211–219, 223–231, 237, 274, 297
cyberwar(fare) 26, 116–117, 118, 120, 124–125, 213, 223

data 8, 9, 10, 23, 30, 64, 95, 99–100, 103, 104, 136, 137, 139, 142, 196, 212, 223–224, 225–226, 226–227, 231, 267, 269, 273–274
democracy 110, 117, 117–120, 121, 122, 123
(co-) design 79, 82, 83, 272
deterrence 9, 13, 19, 20, 23, 27, 30, 52, 78, 94, 180, 251, 252, 256, 285, 300
drone 9, 25, 26, 28, 29, 30, 68, 133, 135–137, 137, 142–152, 182, 224, 269

emic and etic perspective 75, 80–82, 84
emotion 279–290

Hezbollah 24, 50, 142, 146, 268, 296
Houthi(s) 146, 159, 249–259
human decision cycle 93, 94, 97, 110
hybrid warfare 19–20, 45–53

influence 6, 7, 12, 20, 26–27, 29, 30, 47, 59, 66, 72–84, 108, 175, 182, 191, 193, 197, 227–228, 254, 287, 297, 299
information operations (IO) 5, 8, 11, 50, 51, 59–60, 65, 73, 134, 139, 243, 267, 298
information warfare 8, 45, 47, 51, 59, 269, 272, 274–275
institutionalisation 195–197
insurgency 7, 27, 161, 163, 166, 168, 173, 178–179, 196, 249–259, 267, 270, 271

Intelligence Surveillance and Reconnaisance (ISR) 8, 109, 132, 136, 269
International Humanitarian Law (IHL) 211–219, 223, 230, 236–244, 249, 257–258
international law 117, 119, 120–121, 124, 135, 215–216, 219, 226, 249, 252, 253, 254, 257, 259
Iraq 3, 7, 11, 19–20, 22, 23, 25, 27, 50, 73, 74, 131–140, 144, 146, 161–165, 176, 177, 179–180, 181–182, 189–198, 211, 223, 237, 241, 268, 269, 272, 296
Islamic State (IS) 7, 18, 45, 50, 73, 79, 134, 142, 146, 159, 195, 211, 237, 249
Israeli Defence Force (IDF) 50, 224–225, 239, 240, 243

(non-) kinetic 3, 5, 6–7, 11, 13–14, 26, 27, 29, 49, 50, 63, 99, 116–117, 124, 134, 213, 215, 223–224, 225–226, 267, 272, 295–296, 297
Kurdish Democratic Union Party (PYD) 159, 162–165

lawfare 236–237, 243, 244, 249–259, 298
Lebanon 24, 159
Libya 3, 11, 20, 27, 133, 138, 140, 189, 296

machine learning 93–111, 139, 299
manoeuvre 9–10, 12, 13, 134, 173, 241, 268, 271–272, 275, 276, 298
military assistance (MA) 173–177
military innovation 26, 190–191
military objectives 144, 226, 238–240, 242, 251, 255–257
multi-domain operations 8, 138, 267

netwar 272

OODA loop 8, 10, 93–111, 139, 299
operational art 275–276
organisational learning 190–191

political warfare 29, 53, 297–298
precautions attack 216, 219, 228, 236–237, 238–240, 243–244
proportionality 120–121, 216–219, 227–229, 237–238, 240, 242

rebel-system 161–162, 167
remote warfare 176, 182
revolution in military affairs (RMA) 5, 23, 131, 143, 177
Russia 18–22, 28–30, 45–46, 48–50, 72–73, 94, 108, 121, 133, 139, 249, 270, 298, 300

security force assistance (SFA) 7, 65, 173–183, 195, 196, 296
siege 237, 241
social media 24, 28, 29, 50, 58–69, 104, 214, 269, 274, 297
Somalia 144, 145, 159, 178, 179–180
special operations forces (SOF) 80, 133, 173–183, 195, 272
strategic underperformance 17–31
stress 279–290
surrogate warfare 29, 144, 176, 250, 259
synthetic 3, 5, 9–11, 13–14, 138, 270, 295, 299–300
Syria 3, 11, 50, 132, 134–135, 137–138, 144, 146, 159, 161–164, 182, 211, 223, 237, 241, 268, 269, 272, 296

Target Audience Analysis (TAA) 61–66
targeting rules 223–231
technology 3, 6, 10, 11, 12, 29, 47, 52, 72, 93, 96, 107, 116, 119, 131, 137, 140, 142–152, 177–178, 211, 269, 270–273
threshold of attack 211–219

Unmanned Aerial Vehicles (UAVs) 25, 50, 133, 144, 196
urban warfare 236–244

Wagner Group 48
Western way of war 21, 142, 151, 177–178, 182

Yemen 144–145, 159, 237, 250, 253–258